ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

Fakulta biomedicínského inženýrství

Katedra zdravotnických oborů a ochrany obyvatelstva

Terorismus jako významná bezpečnostní hrozba

Terrorism as a Major Security Threat

Diplomová práce

Studijní program: Ochrana obyvatelstva
Studijní obor: Civilní nouzové plánování

Vedoucí práce: doc. PhDr. Marian Brzybohatý, Ph.D.

Mgr. Tomáš Kadubec

Kladno, květen 2017

České vysoké učení technické v Praze, Fakulta biomedicínského inženýrství

Katedra zdravotnických oborů a ochrany obyvatelstva | Akademický rok: 2016/2017

Zadání diplomové práce

Student:	**Bc. Tomáš Kadubec**
Studijní obor:	Civilní nouzové plánování
Téma:	**Terorismus jako významná bezpečnostní hrozba**
Téma anglicky:	Terrorism as a Major Security Threat

Zásady pro vypracování:

Předmětem diplomové práce bude zhodnocení globálního a tuzemského bezpečnostního prostředí s ohledem na zvyšující se riziko teroristických útoků. Cílem diplomové práce bude zhodnotit a porovnat motivy, prostředky a okolnosti teroristických útoků. Komparací útoků minulých a současných bude v práci uvedena predikce dalšího vývoje terorismu jako takového. V souvislosti s výše uvedeným bude v práci věnována pozornost mimo jiné moderním způsobům vedení asymetrického boje a naopak i ochraně před těmito útoky – vyvíjení systémů k ochraně chráněných zájmů. Teoretická část práce bude v analytickém směru primárně věnována typologiím útoků, jejich komparaci a predikci budoucího vývoje. V rámci praktické části bude vypracována případová studie, která v sobě bude zahrnovat projekt, jenž má za úkoly zvýšit bezpečnost vybraných chráněných objektů – zejména vůči kybernetickým útokům a proti zneužití bezpilotních letounů k útokům. Při zpracování práce bude zvolen multioborový přístup k zajištění větší komplexnosti práce.

Seznam odborné literatury:

[1] BRZYBOHATÝ, Marian, Terorismus 2, ed. 1., Praha: Police history, 1999, ISBN 80-902670-4-1
[2] KOVERDYNSKÝ, Bohdan, Letecká security: historie, organizace, standardy a postupy, ed. 1., Cheb: Svět křídel, 2014, ISBN 978-80-87567-51-7
[3] KARAS, Jakub, TICHÝ, Tomáš, Drony, ed. 1., Brno: Computer Press, 2016, ISBN 978-80-251-4680-4
[4] VERTON, Dan, Black Ice: neviditelná hrozba kyberterorizmu, ed. 1., Gliwice: Helion, 2004, ISBN 83-7361-564-4

Vedoucí: doc. PhDr. Marian Brzybohatý, Ph.D.

Zadání platné do: 20.08.2018

..... vedoucí katedry / pracoviště

..... děkan

V Kladně dne 12.12.2016

Prohlášení

Prohlašuji, že jsem diplomovou práci s názvem Terorismus jako významná bezpečnostní hrozba vypracoval samostatně pouze s použitím pramenů, které uvádím v seznamu bibliografických odkazů.

Nemám závažný důvod proti užití tohoto školního díla ve smyslu § 60 zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon).

V Kladně dne 17.05.2017

…….
podpis

Poděkování

Rád bych poděkoval panu doc. PhDr. Marianovi Brzybohatému Ph.D. za odborné vedení, podněty, připomínky při zpracování této diplomové práce a za prokázanou míru pochopení.

Abstrakt

Předmětem diplomové práce je fenomén terorismu v rámci bezpečnostního prostředí. V teoretické části práce je uveden současný stav a vývoj terorismu, společně s jeho historickou klasifikací. Etapizace terorismu má v práci za úkol shrnout minulé i současné problémy a uvést problémy, které se v současné době vyskytují a v budoucnosti budou získávat neustále větší pozornost a budou nabývat na důležitosti.

V rámci dalšího postupu je práce soustředěna na moderní prostředky terorismu – kyberterorismus a využívání bezpilotních letounů (dronů) k páchání teroristických činů. V teoretické části je uveden legislativní základ práce, společně s terminologií, která se k výše uvedeným tématům váže – tedy terorismu, kyberterorismu a využití bezpilotních letounů, jenž slouží k páchání trestné činnosti a teroristických útoků.

Předmětem praktické části práce (výsledky práce) je identifikovat zranitelnosti objektů vůči moderním prostředkům vedení asymetrického boje, zhodnotit současný stav a navrhnout určitá vylepšení a doporučení pro zvýšení bezpečnosti chráněných objektů a zvýšení jejich odolnosti proti takovým hrozbám v budoucnosti.

V rámci diskuze budou porovnány různé přístupy k ochraně objektů před moderními hrozbami, různé pohledy na problematiku terorismu, kyberterorismu a užití bezpilotních letounů v rámci různých společnostní a v odlišném bezpečnostním prostředí.

V neposlední řadě bude zmíněno rozdílně pojetí využití bezpilotních letounů v civilní a vojenské sféře. V souvislosti s tím je nutné brát v potaz i různý systém ochrany, proti různým typům bezpilotních letadel.

Klíčová slova

Terorismus; bezpečnostní prostředí; kyberterorismus; bezpilotní letouny; ochrana objektů; moderní prostředky terorismu

Abstract

The subject of the diploma thesis is the phenomenon of terrorism colliding with the security environment. The theoretical part of the thesis presents the current state and development of terrorism, along with its historical classification. The partition of history of terrorism has the task of summing up past and current problems and presenting current problems that will have greater impact in the future.

As the next step, the thesis is focused on modern means of terrorism - namely cyber-terrorism and the use of unmanned aerial vehicles (drones) to carry out terrorist acts. In the theoretical part, legislative ground for the thesis is presented, along with necessary terminology, which includes terrorism, cyber-terrorism and the use of unmanned aircraft for criminal purposes and terrorist attacks.

The practical part of the thesis is to identify the vulnerability of protected objects against modern means of conducting asymmetric combat, to evaluate the current situation and to propose certain improvements and recommendations for enhancing the safety of protected objects and to increase their resilience against such threats in the future.

In the discussion, different approaches will be compared in ways of protecting objects from modern threats. Different views on the issue of terrorism, cyberterrorism and the use of unmanned aerial vehicle will be described with regard of different companies and in different security environments.

Last but not least, the fact that the concept of use of unmanned airplanes in the civilian and military sectors is be different is noted. In this context, different systems of protection against different types of unmanned aircraft need to be taken into account.

Keywords

Terrorism; Security environment; Cyberterrorism; Unmanned aerial vehicles; Protection of objects; Modern means of terrorism;

Obsah

1 ÚVOD

Diplomová práce se věnuje fenoménu terorismu, který nabývá v současné bezpečnostní situaci stále většího významu a dostává se mu nebývalé mediální a politické pozornosti. Zpracovávané téma jsem si vybral nejen z právě uvedených důvodů, avšak i z důvodu vlastní predikce dalšího nárůstu významu asymetrického boje a v neposlední řadě z důvodu vlastní praxe, kdy jsem od roku 2014 prošel několika úrovněmi zaměstnání v bezpečnostním sektoru a měl možnost sledovat proměnu bezpečnostního prostředí a bezpečnostních opatření v reálném prostředí a čase.

V úvodní části bude zmíněna problematika definice terorismu a jeho interpretace, neboť určitou úpravou definice terorismu lze obsáhnout či vyjmout z této kategorie zkoumané incidenty. Společně s definicí terorismu budou v úvodní části ukotveny další pojmy, které jsou pro další rozvoj práce nutností.

V práci bude současně zkoumána vzrůstající tendence provádění teroristických útoků, jejich motivy a prostředky, kterými jsou útoky prováděny. Mimo jiné bude provedena komparace vývoje prostředků teroristických skupin a predikce možného využití aktuálně vyvíjených technologií k teroristickým útokům.

V praktické části práce bude v rámci případové studie věnován prostor přípravě ochrany chráněných objektů před moderními prostředky, které by mohly být zneužity pro páchání teroristických činů v přítomnosti či budoucnosti.

V průběhu práce budou u daných témat zmíněny i právní dokumenty, které se k problematice váží a upravují bezpečnostní prostředí.

2 SOUČASNÝ STAV

V následující kapitole budou uvedeny základní pojmy a definice, které jsou nutné k základnímu pochopení problematiky terorismu a souvisejících témat. Společně s definicemi bude nastíněno i propojení jednotlivých témat a jejich vývoj.

2.1 Základní pojmy, definice a vybrané právní předpisy

2.1.1 Terorismus

Jak již bylo zmíněno v úvodu práce, pojem terorismus lze obtížně jednoznačně definovat. Pokud je definice obsáhlá či naopak nadmíru obecná, mohou být různé zkoumané incidenty pod akt terorismu špatně zařazeny či naopak nezařazeny. Níže budou uvedeny některé z často užívaných definic.

Jako příklad výše uvedeného problému obtížné definovatelnosti jsou v následující části uvedeny dvě definice, ze stránek MVČR.

Pod prvním odkazem je pojem terorismus definován následovně: *„Terorismus je plánované, promyšlené a politicky motivované násilí, zaměřené proti nezúčastněným osobám, sloužící k dosažení vytčených cílů.“* [1]

Ihned ve stejném článku však lze nalézt další definici, která je širší a byla populární primárně v období let 1980 – 1990, vznikla ve spolupráci FBI a CIA v USA a definuje terorismus následujícím způsobem: *„Terorismus je propočítané použití násilí nebo hrozby násilím, obvykle zaměřené proti nezúčastněným osobám, s cílem vyvolat strach, jehož prostřednictvím jsou dosahovány politické, náboženské nebo ideologické cíle. Terorismus zahrnuje i kriminální zločiny, jež jsou ve své podstatě symbolické a jsou cestou k dosažení jiných cílů, než na které je kriminální čin zaměřen.“* [1]

Je na první pohled zřejmé, že výše uvedené definice se od sebe liší, zejména ve znamení přidružených aktivit – tj. kriminální činnost. Tato problematika bude zmíněna dále v práci v rámci financování teroristických aktivit.

Stále na stejném webu, avšak pomocí jiného odkazu lze nalézt následující definici terorismus: *„Terorismus je politicky, nábožensky či jinak ideologicky motivované násilí. Dle české trestní legislativy je pak definován paragrafem 311 Teroristický útok a paragrafem 312 trestního zákoníku Teror“.* [2]

Z výše uvedené definice je patrné, že i definice uvedené na stránkách MVČR se liší ve své obsáhlosti.

V návaznosti na výše uvedené je dále v trestním zákoníku v paragrafu 129a definována teroristická skupina, v paragrafu 312a účast na teroristické skupině, v paragrafu 312d financování terorismu, v paragrafu 312e propagace terorismu a v paragrafu 312f vyhrožování teroristickým činem. [3]

Výše uvedený výčet není taxativní, neboť dle definic je možné k aktu terorismu přiřadit i další protiprávní činnosti, které slouží jako prostředky k dosažení teroristických cílů – např. dle paragrafu 140 (vražda), dle paragrafu 149 (mučení a jiné nelidské a kruté zacházení), dle paragrafu 172 (zavlečení), dle paragrafu 174 (rukojmí) a dle paragrafu 175 (vydírání), avšak z důvodu uvedení příkladu tuzemské právní úpravy dostačující. [4]

V rámci další ilustrace možnosti definice terorismu jiným způsobem bude uvedena následující definice: *„Terorismus znamená cílevědomé použití násilí páchaného vládními agenty nebo subnárodními skupinami, obvykle proti nebojujícím osobám, za účelem získání pozornosti veřejnosti a jejího následného ovlivňování. V nejobecnější rovině je však terorismus chápán jako forma organizovaného násilí, obvykle*

záměrného proti nezúčastněným osobám, za účelem dosažení politických, kriminálních a jiných cílů.“ [5, s. 8]

Z výše uvedených definic vyplývá, že definování pojmu terorismus může být pojato různým způsobem a posuzování jednotlivých incidentů individuálně zde hraje velkou roli.

V rámci této práce jsou výše uvedené definice a informace dostačující, pro další prohloubení znalostí autor doporučuje prostudovat např. Bezpečnostní strategii 2015, zprávu EU o teroristické situaci a bezpečnostních trendech (Europol TE-SAT report), která byla vydána pod organizací Europol, strategii České republiky pro boj proti terorismu od r. 2013 či další související dokumenty. V uvedených dokumentech jsou uvedeny nové hrozby a bezpečnostní postupy, jak se na tyto hrozby připravit.

2.1.2 Vývoj terorismu

Historie lidského pokolení jde ruku v ruce s historií válek a ozbrojených konfliktů. Téměř každý konflikt v historii je spojen se zásahem do životů civilního obyvatelstva. I když se v průběhu historie snažily mocné osoby (panovníci či i demokratičtí vůdci) redukovat počet civilních obětí, neboť to je i v jejich zájmu, civilní oběti v ozbrojených konfliktech byly, jsou a budou. V určité míře je totiž násilí nediskriminující. Teror páchaný na civilním obyvatelstvu byl a dodnes je takřka nedílnou součástí konfliktního chování osob při moci či civilizací (náboženské konflikty apod.) [6]

Jako zásadní zlom ve vývoji terorismu lze identifikovat moment, kdy formy terorismu začaly být využívány jako prostředky k dosažení cílů jednotlivých skupin za pomoci vyvíjení tlaku na odpovědné osoby s cílem změnit jejich chování, i když dle předchozích určených pravidel neměly

dostatek moci ani prostředků k vyvolání takové změny. Teroristé tedy začali využívat útoky k propagování svého cíle a využívali strachu jako nosiče svého poselství. V rámci tohoto zlomu byly za tyto taktiky již zodpovědné teroristické skupiny, v aktuální podobě se jedná o terorismus mezinárodní, resp. globální. [6]

Identifikovat počátek samotného terorismu lze velmi obtížně. J. Šedivý (bývalý náčelník Generálního štábu české armády) uvádí jako první etapu terorismu prehistorickou fázi, kam zařazuje vraždy tyranů a despotických vládců ve starověkém Řecku a Římě, akce islámských hašašínů v období křižáckých válek a další. Další etapu považuje propuknutí anarchistických, nihilistických a nacionalistických hnutí na konci 19. století, kde útoky páchali převážně jedinci. Jako příklady uvádí zavraždění ruského cara, amerického prezidenta a mnohé další, avšak zdůrazňuje i fakt, že ne všechny uvedené příklady zapadají do prvotního vymezení terorismu. Jako konec této etapy označuje útok na Františka Ferdinanda d'Este v roce 1914. Další etapu označuje jako studenoválečnou, která je zasazená do období po druhé světové válce. Jako příčinu zde uvádí úsilí o marxistickou orientaci a snahu přeměny společnosti na Středním východě, v Jižní Americe a v určitých regionech Afriky. [7]

Výše uvedená etapizace slouží jako základní rozdělení vývoje terorismu, avšak s jeho rozvojem je nutná jeho další rozdělení a začlenění i aktuálních událostí. Foltin a Řehák klasifikují vývojové etapy následujícím způsobem:

1) *„Historická etapa – trvající do konce 17. století;*
2) *Nacionalistická etapa – probíhající od počátku 18. století až do roku 1913;*
3) *Etapa válek – probíhající v letech 1914 až 1945;*
4) *Etapa studené války – probíhající od roku 1946 až do roku 1989;*

5) *Etapa studeného míru – trvající od roku 1990 až po současnost"* [8, s. 47]

Autor práce by uvedenou etapizaci upravil a přidal 6. etapu, která by reflektovala moderní dobu, kde se zvyšuje význam medializace útoků, sociálních sítí, informačních technologií a k nim vázajícím se fenomén kyberterorismu. V době sestavování výše uvedené etapizace však nebyl kybernetický prostoj rozvinutý do takové míry, jako je tomu dnes, tím pádem pochopitelné, že etapizace nereflektuje současné moderní problémy. Fenoménu kyberterorismu bude blíže popsán v následujících kapitolách.

2.1.3 Kyberterorismus

V odborné literatuře je možné najít definice týkající se problematiky kyberterorismu. Do této práce byl pro ilustraci však vybrán omezený počet definic tohoto fenoménu. Škála definic se rozpíná od nejobecnějších forem, jaké lze zkonstruovat, které jsou určeny pro zjednodušení problematiky a z důvodu pochopitelnosti i pro čtenáře, který není odborníkem v oblasti informačních technologií. Přes sporné formy, které samy zpochybňují určité aspekty problematiky kyberterorismu, až po poměrně komplexní formy, které se snaží obsáhnout celou problematiku a zohledňují více úhlů pohledu.

V rámci zpracovávaného tématu zde bude uveden zástupce zahraniční definice, a též zástupce definice tuzemské, z důvodu ilustrace různého pojetí problematiky. V rámci ČR je důležité zmínit, že problematika kyberterorismu je povrchově obsažena i v typovém plánu: narušování zákonnosti velkého rozsahu.

Níže bude uvedena definice, kterou lze nalézt na stránkách Ministerstva vnitra ČR, který se dá považovat za velmi úzkou, avšak je také dostatečně

obecná pro obsáhnutí širokých kritérií problematiky a je v ní uveden i termín „kyberprostor“.

„Kyberterorismus je souhrnný název pro teroristické aktivity, jejichž cílem útoku, použitým prostředkem nebo přenašečem je tzv. „kyberprostor“, neboli jde o teroristické aktivity zaměřené proti a prováděné prostřednictvím počítačové sítě a touto sítí řízených systémů („informační elektronické síťové struktury“).“ [9]

Je možné nalézt další definice, které například považují kyberterorismus za sporný termín. Někteří autoři si vybírají velmi úzké definice, opírající se o provádění kybernetických útoků v rámci známých teroristických organizací. Staví na základě jejich útoků proti informačním systémům a za jejich primární účel staví vytvoření strachu a paniky. V rámci těchto úzkých definic je však obtížné obsáhnout všechny instance kyberterorismu. [10, s. 137]

„Kyberterorismus je konvergencí terorismu a kyberprostoru, obecně chápaný jako nezákonný útok nebo nebezpečí útoku proti počítačům, počítačovým sítím a informacím v nich skladovaným v případě, že útok je konán za účelem zastrašit nebo donutit vládu, nebo obyvatele k podporování sociálních nebo politických cílů.“ [11]

Výše uvedená definice je výstižná a proto při zmínce o kyberterorismu budu odkazovat právě na ní.

K pochopení problematiky kyberterorismu je nutné uvést další související definice, které se při zkoumání tohoto fenoménu vyskytují. Výběr definic rozhodně není taxativní, jedná se pouze o vybrané pojmy používané v této práci či v bezpečnostní terminologii, které jsou:

- Kybernetickým prostorem se míní digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy,

a službami a sítěmi elektronických komunikací. [12]

- Kritická informační infrastruktura je vnímána jako prvek nebo systém prvků kritické infrastruktury v odvětví komunikační a informační systémy v oblasti kybernetické bezpečnosti. [12]
- Hrozbou je míněna potencionální příčina kybernetické bezpečnostní události nebo kybernetického bezpečnostního incidentu, jejímž výsledkem může být poškození aktiva. [13]
- Zranitelností je míněno slabé místo aktiva nebo bezpečnostního opatření, které může být zneužito jednou nebo více hrozbami.
- Kybernetická bezpečnost je de facto souhrn právních, organizačních, technických a vzdělávacích prostředků směřující k zajištění ochrany kybernetického prostoru.
- Správcem informačního systému veřejné správy subjekt, který podle zákona určuje účel a prostředky zpracování informací a za informační systém odpovídá. [12]
- Informačním systémem se rozumí funkční celek nebo jeho část zabezpečující cílevědomou a systematickou informační činnost. Každý informační systém zahrnuje data, která jsou uspořádána tak, aby bylo možné jejich zpracování a zpřístupnění, a dále nástroje umožňující výkon informačních činností. [14]

Výčet pojmů není taxativní, výše jsou uvedeny pouze základní termíny, které se budou v práci objevovat. Další terminologie bude v práci uvedena průběžně u probíraných témat.

2.1.4 Propojení kybernetického prostoru a teroristických útoků

Šíření a rozrůstání kybernetické kriminality společně s profesionalizací podsvětní ekonomiky, která je založená na systému výměny (elektronická měna – BitCoin apod.), jenž se dá obtížně sledovat a vede ke snížení požadavků na

technickou zdatnost zločinců a útočníků, vede ke zjednodušení zajištění potřebných služeb a nástrojů, které potřebují útočníci k provádění svých nezákonných činností. [15]

Utajování nezákonných činností, vlastní identity a činnosti spojené s praním špinavých peněz, jakož i nákup střelných zbraní a výbušnin je v tomto prostředí anonymnější a do jisté míry i jednodušší. Právě anonymita, jednoduchost a snazší dostupnost jsou faktory, které mohou kybernetické prostředí zpřístupňovat teroristům. Jelikož se technická kapacita v rámci teroristických skupin neustále zvyšuje, lze předpokládat, že model Zločin jako služba (Crime-as-Service (CaaS)) by se mohl rozšířit i na terorismus.

Vzhledem k tomu, že dochází k rozmazávání hranice mezi užíváním nástrojů a technik k teroristickým útokům a mezi kybernetickými útočníky těmi, kteří používají kybernetické prostředky „pouze" k nelegálnímu získání finančních prostředků, je také pravděpodobné, že teroristé budou získávat stále pokročilejší nástroje k páchání kybernetických útoků, které budou obtížněji odhalitelné. Nárůst této hrozby je obzvlášť závažný, pokud se to týká kritické infrastruktury. Jeden ze scénářů možného útoku na kritickou infrastrukturu by mohl například zahrnovat masivní útok DDoS (Distributed Denial of Service) s cílem narušit kritickou infrastrukturu. [15]

Pokud jde o zneužívání šifrování a zajištění anonymity, zdá se, že teroristické skupiny jako IS se v tomto ohledu neustále zdokonalují. Al-kaida například využívá vlastní šifrovací software, Asrar al Mujahedeen (Mujahedeenovo tajemství), v manifestu Anders Breivika, lze nalézt podrobný návod jak používat prohlížeč TOR (The Onion Router) a jak využívat virtuální privátní sítě (VPN) k zajištění anonymity. Skutečnost, že IS má v oblibě využívat otevřené aplikace pro zabezpečení komunikace, jako je například

aplikace Telegram a používá kanálů Darknet k nákupu střelných zbraní jsou jasným indikátorem, že teroristé si jsou možností využití kybernetických prostředků vědomi, aktivně je využívají a jejich využívání se bude do budoucnosti zefektivňovat. [15]

Stejně jako u ostatních (neteroristických) kybernetických trestných činů jsou teroristé schopni pracovat ze vzdálených míst a minimalizovat riziko detekce způsobené cestováním nebo přípravou útoku v cílové zemi.

Kybernetické útoky mohou být vedeny na informační infrastrukturu z různých důvodů a na různé oblasti. Např. s cílem ochromení bezpečnostních složek či narušení dopravních kapacit. V následujícím obrázku budou zobrazeny různé typy útočníků a jejich motivace.

Je proto důležité zvážit pravděpodobnost, že budoucí útoky budou založeny na novém MO (modus operandi) se silnějším kybernetickým rozměrem. Teroristé v současné době demonstrují svou flexibilitu a ochotu učit se a dále rozvíjet své technické dovednosti, bezpečnostní složky musí adekvátně reagovat. [15]

2.1.5 Bezpilotní letouny – drony

Bezpilotní letouny (UAV), také známé pod označením drony, jsou letouny bez lidského pilota na palubě. [16]

Bezpilotní letouny mohou pracovat s různým stupněm autonomie - buď pod dálkovým ovládáním člověka, nebo autonomně ve spolupráci s palubními počítači. Autonomní drony představují vyšší stupeň ohrožení, neboť některé systémy, které mají zamezit využití dronů jsou proti těmto typům neúčinné, neboť se zaměřují na inhibici spojení mezi dronem a operátorem, které zde není.

Původním smyslem dronů bylo operovat v místech, které bylo pro letoun s pilotem nebezpečné. Avšak v průběhu výzkumu si drony našli cestu do mnoha odvětví – od zemědělského a průmyslového využití, přes sledování osob, pašování drog, doručování zásilek až po sportovní disciplíny – např. závody dronů.

V rámci definice dronů lze definovat bezpilotní letadla následujícím způsobem: *„Drony jsou leteckým prostředkem, který nenese lidského operátora, využívá aerodynamické síly ke vzlétnutí, může letět autonomně nebo může být pilotován vzdáleně, může být určen k jednotlivému využití nebo být využit opakovaně a může nést smrtelné nebo paralyzující prostředky.“* [17]

Je mnoho druhů klasifikací bezpilotních letounů, pro účely práce zde bude uvedeno základní rozdělení podle účelu:

- **Drony jako cíl a návnada** - poskytuje pozemním a leteckým zbraňovým systémům cíl, který simuluje nepřátelské letadlo nebo střely – přitahuje k sobě nepřátelské střely a snižuje riziko zasáhnutí cílů s lidskou posádkou.
- **Drony určené k průzkumu** – poskytuje informace z bojiště – počet nepřátel, jejich výzbroj, optimální postup jednotek apod.
- **Drony určené pro boj** – poskytují palebnou podporu jednotkám v rámci vysoce rizikových misích, je možné je využít jako samostatné zbraňové platformy. Například drony typu Reaper MQ-9 – více v praktické části práce.
- **Logistické drony** - slouží k dodání materiálu na určené místo
- **Drony určené k výzkumu a vývoji bezpilotní technologie** – experimentální drony, které rozvíjí schopnosti současných dronů a později jsou aplikovány do běžného užívání.

- **Drony určené k civilnímu užití a k obchodu** – lze najít uplatnění v zemědělství, pořizování fotografií z ptačí perspektivy se sníženou cenou na pořízení, sběr dat pro průmyslové účely a mnoho dalších. [17]

Další systémy klasifikace mohou brát jako kritérium pro dělení např. váhu bezpilotního letounu, výšku, v které operuje, jeho zjistitelnost specializovanou technikou. Výčet není taxativní a do budoucna se bude zcela jistě rozšiřovat. V rámci práce bude však výše zmíněné dělení dostačující.

2.1.6 Vybrané právní předpisy

V následující části budou uvedeny vybrané právní předpisy platné v rámci ČR a zároveň i mezinárodní koncepční dokumenty dle jednotlivých témat, na které se práce zaměřuje.

2.1.6.1 Právní dokumenty – terorismus

V rámci ČR je problematika kyberterorismu upravena v následujících dokumentech a předpisech.

Tabulka 1 Právní předpisy upravující terorismus v rámci ČR [18, 19, 20, vlastní tvorba]

Dokument / právní předpis	*Obsah dokumentu / právního předpisu*
Strategie České republiky pro boj proti terorismu od r. 2013	Dokument klade důraz na: • Zlepšení komunikace a spolupráce mezi subjekty, zapojenými do boje proti terorismu. • Legislativní a mezinárodně-smluvní otázky. • Ochranu obyvatelstva, kritické infrastruktury a jiných cílů, potenciálně zranitelných teroristickým

	útokem. • Bezpečnostní výzkum, vzdělávání a informování veřejnosti ve vztahu ke konkrétním aspektům boje proti terorismu. • Prevenci radikalizace ve společnosti a boji proti rekrutování do teroristických struktur.
Zákon č. 40/2009 Sb. trestní zákoník	V trestním zákoníku je definován teroristický útok (§311), Teror (§312), teroristická skupina (§129a), účast na teroristické skupině (§312a), financování terorismu (§312d), propagace terorismu (§312e), vyhrožování teroristickým činem (§312f) – ukládá tresty a jejich délku.
Zákon č. 418/2011 Sb., o trestní odpovědnosti právnických osob a řízení proti nim	Obsahuje zavedení trestní odpovědnosti právnických osob do právního řádu členských států. Možno stíhat právnické osoby kvůli teroristickým činům, podpoře terorismu a dalším souvisejícím činům. Zavedeno Rámcového rozhodnutí Evropské unie o boji proti terorismu (2002/475/SVV).
Usnesení vlády české republiky ze dne: 13. Září 2006 č. 1060	Obsahuje zásady koordinace činnosti zpravodajských služeb České republiky při vyhodnocování informací důležitých pro bezpečnost České republiky se zvláštním zaměřením na boj proti terorismu – dochází zde k zavedení předávání informací získané členy Vojenského zpravodajství a Úřadu pro zahraniční styky a informace do kompetence bezpečnostní informační služby (BIS).

Zákon č. 153/1994 Sb., o zpravodajských službách České republiky	Tento dokument upravuje především postavení, působnost, koordinaci, spolupráci a kontrolu zpravodajských služeb České republiky - § 5 odst. 1 písm. e – definuje působnost a povinnost BIS zabezpečovat informace týkající se organizovaného zločinu a terorismu.

Existuje samozřejmě celá řada právních předpisů a dokumentů, které upravují v rámci svých působností problematiku terorismu, buď přímo či nepřímo např. (zásady koncepce integrace cizinců na území České republiky, postup při realizaci Koncepce integrace cizinců apod.), avšak pro účely této práce je tento výčet dostačující.

Další uvedené dokumenty jsou mezinárodního charakteru, avšak pro jejich počet a rozsáhlost budou uvedeny jen některé z nich.

Tabulka 2 Mezinárodní právní předpisy upravující terorismus [21, 22, vlastní tvorba]

Dokument / právní předpis	*Obsah dokumentu / právního předpisu*
Rámcové rozhodnutí Evropské unie o boji proti terorismu (2002/475/SVV)	Dokument, který mimo jiné výslovně vyžaduje zavedení trestní odpovědnosti právnických osob do právního řádu členských států.
Evropské strategie proti radikalizaci	Upravuje prostředí a uplatňuje se především ve věznicích a prostřednictvím internetu.

Strategii vnitřní bezpečnosti EU	Definuje nutnost propojení bezpečnostních systémů jednotlivých členů EU, prosazuje jednotný model bezpečnosti.
Strategie EU pro boj proti terorismu	Obsahuje především snahy definované jako: • Předcházení radikalizace a náboru teroristů. • Ochrana občanů a infastruktury. • Pronásledování teroristů přeshraničně s cílem narušit plánování a financování jejich útoků. • Reagování na následky teroristických akcí.
Europol TE-SAT report	Obsahuje nejnovější trendy, počet odhalených a provedených útoků, statistiky útoků, nové prostředky, úsilí v boji proti terorismu a mnoho dalšího.

Komparací mezinárodních a tuzemských právních předpisů a dokumentů lze získat jejich charakteristiku a ta je taková, že mezinárodní předpisy se soustředí na podněcování spolupráce mezi státy a složkami jejich bezpečnostních systémů – de facto se jedná převážně o strategické dokumenty. Na druhou stranu tuzemská úprava se soustředí na faktickou právní úpravu, provádění opatření a úkony k represi teroristických aktivit.

2.1.6.2 Právní dokumenty – kyberterorismus

Jako legislativní základ diplomové práce v oblasti kyberterorismu se budou využívat následující právní předpisy – tedy převážně zákony, vyhlášky

a nařízení, které byly vyprodukovány v rámci ČR i v zahraničí. Tuzemské zákony vznikly jako výsledek spolupráce s organizacemi a státy, které již dříve obdobnou legislativu implementovali (NATO, EU,…).

Tabulka 3 Právní předpisy upravující kyberterorismus v rámci ČR [23, 24, 25, 26, vlastní tvorba]

Dokument / právní předpis	*Obsah dokumentu / právního předpisu*
Zákon č. 181/2014 Sb., o kybernetické bezpečnosti	Obsahuje vymezení důležitých pojmů pro oblast kyberprostoru, povinnosti pro organizace, kterých se kybernetická ochrana týká, systém opatření, stav kybernetického nebezpečí, systém kontroly a další.
Zákon č. 365/2000 Sb., o informačních systémech veřejné správy	V tomto právním předpisu jsou obsažena práva a povinnosti, které souvisejí s vytvářením, užíváním, provozem a rozvojem informačních systémů veřejné správy. Jsou zde vymezené pojmy IS, systém kontroly, akreditace a další.
Zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů.	Tento právní předpis má především regulační charakter, má za úkol narovnávat hospodářské prostředí. Co se týče bezpečnosti a terorismu, je zde upraven odposlech a záznam zpráv pro odhalování hrozeb – týká se to především BIS a Vojenského zpravodajství. Dále je zde definována bezpečnost a integrita veřejných sítí a prostředků elektronické komunikace a povinnosti provozovatelů – např. stanovení ochranných pásem.
Vyhláška č. 316/2014	Tato vyhláška stanoví obsah a strukturu

Sb., o kybernetické bezpečnosti	bezpečnostní dokumentace pro informační systém kritické informační infrastruktury, komunikační systém kritické informační infrastruktury nebo významný informační systém, obsah bezpečnostních opatření, typy a kategorie bezpečnostních incidentů, náležitosti a způsob hlášení kybernetického bezpečnostního incidentu, náležitosti oznámení o provedení reaktivních opatření. [25]. Tato vyhláška již podle svého názvu řeší „agendu“ kybernetické bezpečnosti (upřesňuje, co přesně by povinné subjekty měly dělat), ale sama neřeší, které subjekty to budou.
Nařízení vlády č.315/2014 Sb., kterým se mění nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury	Zde jsou definovány kritéria pro definování kritické informační infrastruktury a nově je zde uvedena oblast kybernetické bezpečnosti, kde jsou uvedeny časové, osobnostní a průtokové limity informačních sítí.
Národní strategie kybernetické bezpečnosti České republiky na období let 2015 až 2020	V tomto dokumentu jsou definovány vize kybernetické bezpečnosti, tým GovCERT, principy kybernetické ochrany, rozvoj kapacit, a výzvy s kterými se musí bezpečnostní experti a společnost potýkat a hlavní cíle strategie a implementace akční plánu, který ze strategie vychází. [26]
Akční plán k Národní	Tento dokument aplikuje Národní strategii

strategii kybernetické bezpečnosti České republiky na období let 2015 až 2020	kybernetické bezpečnosti České republiky na období let 2015 až 2020 a přiřazuje ji jmenovitě úkoly a časový rámec, v kterém musí být dané úkoly splněny – obvykle v čtvrtletní periodě.

Jako příklad mezinárodních smluv o kybernetické kriminalitě se dá uvést např. Úmluva o kybernetické kriminalitě (2001). Tato úmluva měla především za úkol rozvíjet mezinárodní spolupráci v oblasti kybernetické bezpečnosti.

Inovativním právním dokumentem, který se váže k problému „kybernetické války“, je tzv. Tallinský manuál (Resp. jeho verze 2.0, která byla vydán v roce 2016 prostřednictvím nakladatelství Cambridge University Press), jedná se doposud o jeden z nejvýznamnějších dokumentů, který mapuje pohled mezinárodní právní úpravy na nový typ války.

Tato příručka mezinárodního práva, která je aplikovatelná na „kyberválku“ sestavil soubor dvaceti nezávislých expertů pro NATO. Nejedná se o oficiální stanovisko, ale vypovídá jako sonda současného pohledu na nový typ formující se války. [27]

Tallinn 2.0, který je upravenou verzí originálního manuálu, je sestaven tak, aby rozšířil rozsah původního Tallinnského manuálu, v podstatě je Tallinn 2.0 druhou edicí prvního manuálu.

Primární zaměření původního Tallinnského manuálu jsou nejvíce rušivé a destruktivní kybernetické operace, které kvalifikují jako "ozbrojené útoky", a ve výsledku dává státům možnost reagovat v sebeobraně na kybernetické útoky, které probíhají v průběhu ozbrojeného konfliktu či mimo něj. Vzhledem k tomu, že hrozba kybernetických útoků nabývá na aktuálnosti a vážnosti, se

tomuto tématu věnuje neustále vetší pozornost a vědecká obec a odborníci se, stejně jako tento dokument, začíná na problematiku kybernetických útoků více zaměřovat.

Státy po celém světě čelí (především ve vyspělých zemích) v současné době každý den kybernetickým útokům v různých formách, které neustále nabývají na vážnosti a na sofistikovanosti. Projekt Tallinn 2.0 zkoumá mezinárodní právní rámec, který se vztahuje k výše uvedeným kybernetickým útokům. Příslušné právní režimy obsažené v dokumentu zahrnují vnitrostátní právní úpravy států, právní úpravu na moři, mezinárodní telekomunikační právo, práva kosmického prostoru, diplomatické a konzulární právo atd. Tallinn 2.0 také zkoumá, jaké jsou obecné zásady mezinárodního práva, mezi ně se řadí svrchovanost, právní příslušnost, due diligence (angloamerický právní institut vyjadřující míru aktivity, kterou lze důvodně očekávat za daných okolností) a zákazy intervence a jejich užití, uplatnění v kybernetickém kontextu. [28]

Dalším příkladem může být Národní strategie kybernetické bezpečnosti na období let 2016 – 2021 (National Cyber Security Strategy 2016 to 2021 – UK), která je modernější obdobou naší strategie, má podobnou, avšak graficky jinak řešenou strukturu a soustředí se mimo vizí a cílů i na osvětu a předání informací i neodborné veřejnosti. Dále uvádí i typy útoků s příklady a problémy s kterými se bezpečností složky potýkají. Dále definuje doporučení pro skupiny ve společnosti a stejně jako naše strategie představuje svůj akční plán, který je na rozdíl od strategie ČR zakomponován přímo do strategie. [29]

Výše uvedené právní předpisy jsou pouze výběrovým přehledem a v práci budou případné další právní předpisy zmíněny u témat relevantně.

Při provedení komparace je možné pozorovat opakování trendu mezinárodních dokumentů být více koncepčního a strategického charakteru, avšak v tomto případě i tuzemská úprava dává důraz na spolupráci dotčených složek.

2.1.6.3 Právní dokumenty – bezpilotní letouny

V rámci následující podkapitoly jsou zmapovány právní předpisy a dokumenty týkající se bezpilotních letounů, jejich obsluhy, omezení a podmínek provozu.

Tabulka 4 Právní předpisy upravující problematiku bezpilotních letounů v rámci ČR [30, 31, 32, 33, vlastní tvorba]

Dokument / právní předpis	*Obsah dokumentu / právního předpisu*
Zákon č. 49/1997 Sb., o civilním letectví ve znění pozdějších přepisů	Tento právní předpis upravuje proces získání povolení k létání letadla bez pilota na palubě (§ 52) a získání povolení k provozování leteckých prací (§ 73) nebo leteckých činností pro vlastní potřebu (§ 76) – mapuje hlavně proces získání oprávnění k provozování bezpilotního systému.
Letecký předpis řady L - L2 (na základě Chicagské smlouva a postupů ICAO)	Obsahuje pravidla pro provozování bezpilotních letounů – jmenovitě v Doplňku X, kde jsou uvedené definice bezpilotních letounů, rozsah působnosti, bezpečnost, odpovědnost, dohled pilota, prostory k létání a další podmínky.
Zákon č. 101/200Sb., o ochraně osobních údajů a specifické	Upravuje podmínky pořizování záznamů během letu dronu, např. zakazuje pořizování snímků soukromých aktivit ostatních občanů bez jejich

stanovisko Úřadu pro ochranu osobních údajů 1/2013	souhlasu (zejména v rámci jejich obydlí). A naopak určuje, za jakých podmínek pořizovat může.

Tabulka 5 Mezinárodní předpisy upravující problematiku bezpilotních letounů v rámci ČR [34, 35, vlastní tvorba]

Dokument / právní předpis	*Obsah dokumentu / právního předpisu*
Dokument D122 Evropské komise 8/4/2014	Definuje typy bezpilotních letounů (dálkově řízený / bezobslužný systém), činnosti, ke kterým jsou drony využívány, velikost trhu s drony, pravidla pro konstrukci, organizace pro regulaci (ICAO, EASA), současné problémy a pravidla provozování.
Nařízení Evropského parlamentu a Rady (ES) č. 785/2004	Stanovuje povinnost pojištění dronů k uhrazení škody spáchané třetím osobám. Vyžaduje nutnost začlenění této povinnosti do právních předpisů jednotlivých členu EU.

Komparace mezinárodní právní úpravy a tuzemské právní úpravy již není v oblasti bezpilotních letounů tak rozdílná, jako je tomu u témat kybernetické ochrany a terorismu. Mezinárodní úprava stále řeší více strategická témata, avšak detailněji se vyjadřuje i k jednotlivým problémům, což řeší i úprava na úrovni jednotlivých států. V současnosti se právní úprava neustále vyvíjí a adaptuje, neboť oblast bezpilotních letounu je velmi proměnlivá a je třeba neustále reagovat na změny a inovace v odvětví. V rámci mezinárodní úpravy je třeba zvýraznit úlohu mezinárodních organizací jako je ICAO, EASA a FAA

(federální letecká správa), neboť právě tyto organizace ovlivňují prostředí, ve kterém mohou bezpilotní letouny vzkvétat.

3 CÍLE PRÁCE A HYPOTÉZY

3.1 Cíle práce

V teoretické části práce byl definován terorismus a jeho moderní formy, prostředky a právní úprava v rámci ČR ve spojení s mezinárodním prostředím. Na tento základ naváže část praktická (výsledky práce), kde budou identifikovány stávající problémy týkající se převážně moderních forem teroristických útoků a navrhnuty vylepšení, které při správné aplikaci povedou ke snížení rizika a snížení potencionálních ztrát, které by vznikly v případě útoků.

Cílem práce je tedy navrhnout účinná opatření či doporučení k zavedení nových systémů, postupů, výcviku či úprava současných systémů k ochraně objektů před kybernetickými útoky a teroristickými útoky prostřednictvím bezpilotních letounů.

Ochrana před výše uvedenými útoky bude do budoucna důležitou složkou bezpečnosti a rizika z nich plynoucí uvádí např. portál security guide následujícím způsobem*: "Správné nasazení bezpilotních letounů (UAV – Unmanned Aerial Vehicle) či dronů umožňuje velkou podporu pro vojenské a vládní akce a dohled nad zákonem. Zároveň mohou tato zařízení představovat velká nebezpečí pro leteckou dopravu, snadno je lze použít pro zločinné úmysly, případně teroristické akce."* [36] Z tohoto důvodu shledávám zkoumání daného tématu za podnětné a cíle práce oprávněné.

3.2 Hypotézy

V rámci diplomové práce bude ověřena platnost následujících hypotéz:

1. Ochrana proti moderním prostředkům páchání teroristických činů vůči chráněným objektům není adekvátní a vyžaduje vylepšení.
2. Vzhledem k neustálému technologickému pokroku roste možnost využívání bezpilotních letounů a je třeba tuto oblast regulovat.
3. Moderním prostředkům páchání teroristických činů je nutno věnovat v rámci ČR i v mezinárodním rámci stále větší pozornost a je nutné přijímají adekvátní opatření.

4 METODIKA

V rámci teoretické části práce byly definovány základní pojmy a uvedeny vybrané relevantní právní předpisy za pomoci literární rešerše. Teoretická část obsahuje převážně informace o fenoménu terorismu, včetně jeho moderních forem a vybraných prostředků, které se k teroristickým činům dají využít. Jako zdroj posloužily především odborné monografie, tuzemské i zahraniční právní předpisy, odborné články, koncepční dokumenty, oficiální internetové stránky ministerstev a dalších subjektů, které mají k problematice terorismu vztah. V teoretické části je také využito komparace při srovnání mezinárodních a tuzemských právních předpisů a znázorněn rozdíl mezi nimi. [37]

V následující praktické části bude také využita literární rešerše, kde budou využity zahraniční a tuzemské prameny. Společně s literární rešerší bude dále využívána metoda komparace v případě porovnávání vhodnosti jednotlivých řešení pro identifikované problémy. Dále bude využívána analýza a syntéza. Analýzou bude proveden rozklad problémů kybernetické bezpečnosti a užívání bezpilotních letounů k útokům a obrany vůči nim. U identifikovaných problémů bude navrhnuto optimální řešení, či poskytnuty možnosti, jak problém vyřešit. Další využitou metodou bude syntéza, která spojí získané poznatky z analýzy a rešerše k vyvození adekvátních závěrů. [38]

Práce bude také obsahovat prognózu možného budoucího vývoje zkoumané oblasti a problémů. Tato prognóza bude vycházet z analýzy současného bezpečnostního prostředí, zkoumání tuzemské i zahraniční literatury a právních předpisů a v neposlední řadě aktuálních trendů a technologických inovací.

V průběhu práce bude společně s výše využívanými metodami využita interpretace (převážně u právních předpisů, koncepcí a výkladů). Dále bude

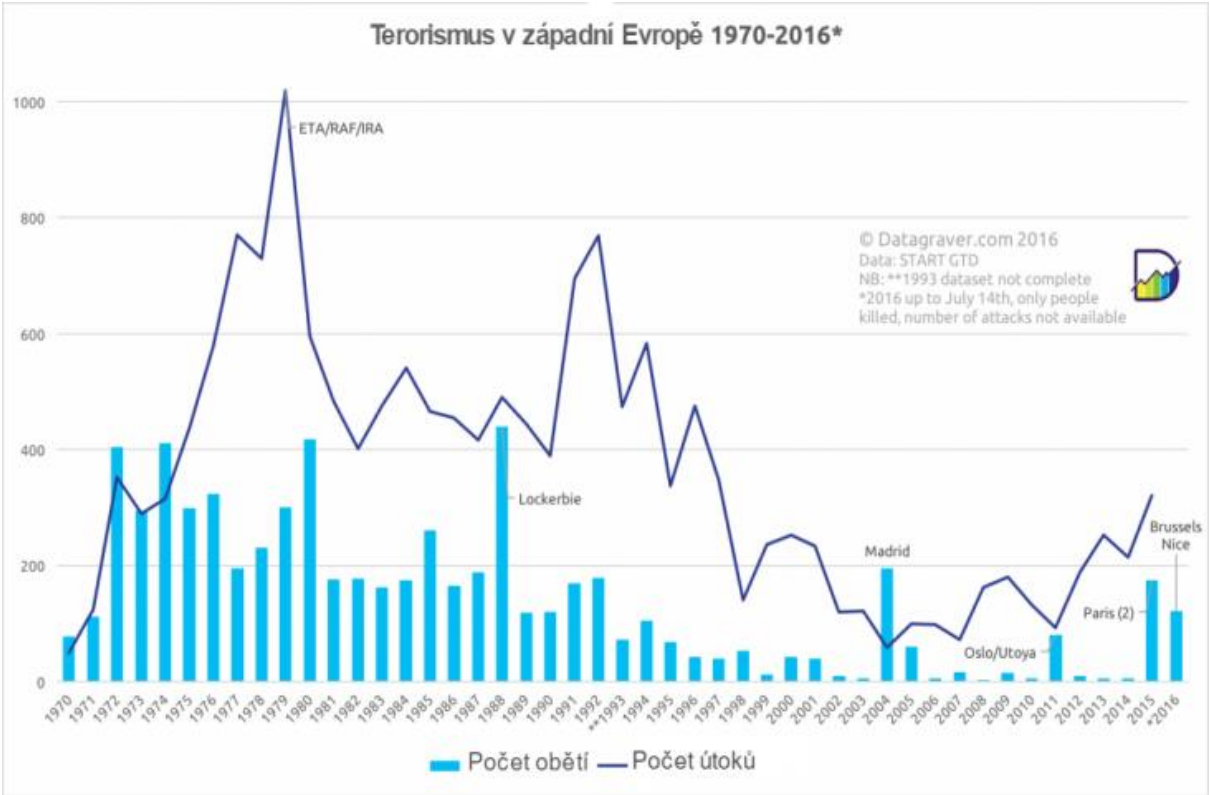
využit řízený rozhovor, kde autor získával informace od pracovníků odpovědných za kybernetickou bezpečnost v rámci společnosti v které je aktuálně zaměstnán – tyto informace budou volnou formou zakomponovány do práce a zejména v rámci identifikace problémů kybernetické bezpečnosti a jejich řešení. Za pomocí kompilace budou setříděny poznatky z většího počtu zdrojů a budou sjednoceny do uceleného textu. V neposlední řadě je využita metoda pozorování, kde autor využije poznatky získané v průběhu svého zaměstnání na různých pozicích v bezpečnostním sektoru.

Dále budou sestaveny případové studie, týkající se kybernetické bezpečnosti, kdy bude vždy definován stav, označen původce útoku a následek útoku. Na případové studie bude navazovat koncepční projektem ochrany chráněných objektů proti bezpilotním letounům. Všechny výše uvedené metody budou využity k potvrzení či vyvrácení stanovených hypotéz a ke tvorbě uceleného závěru s návrhem opatření ke zlepšení současného stavu.

5 VÝSLEDKY PRÁCE – PRAKTICKÁ ČÁST

5.1 Vývoj a aktuální stav terorismu v západní Evropě

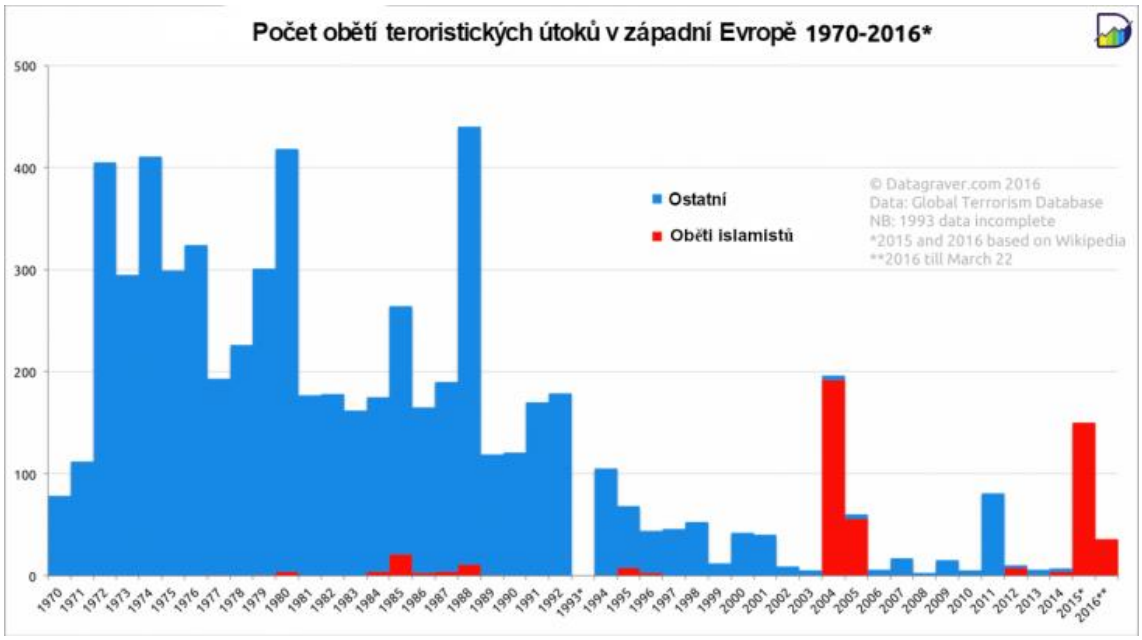
V následující kapitole bude znázorněn vývoj, aktuální stav a predikce zvyšování či snižování frekvence teroristických útoků v regionu, který je mediálně hustě pokryt a osobně se dotýká naší společnosti – tedy západní Evropě. Právě média dávají terorismu a zejména pak modernímu terorismu svoji sílu či jeho dopady umocňují. Z výstupu z následujících grafů bude zkonstruován závěr o nárůstu či poklesu šance na zásah ČR a dalších evropských zemi teroristickými útoky.



Graf 1 – Vývoj terorismus v západní Evropě (1970 – 2016) [39]

Z uvedeného grafu vyplývá, že aktuálně dosahují v západní Evropě teroristické tendence nárůstu a v dohledné době tomu nejspíše nebude jinak.

Při hledání příčiny a je za vhodno zkoumat dřívější útoky a útoky současné. Pro tento úkol bude využit další graf, který znázorňuje počet obětí při teroristických útocích, stejně jako graf předchozí, avšak jsou rozlišeny na ostatní oběti a oběti islamistů.



Graf 2 – Počet obětí teroristických obětí v západní Evropě (1970 – 2016) [39]

Z grafu je zřejmé, že v posledních letech jsou pachatelé teroristických činů v západní Evropě islamisté. V grafu nejsou započítány oběti po březnu 2016 a v roce 2017, které by v západní Evropě do statistiky přidali další oběti skupině islamistických útočníků. Vzhledem k nepokojům v zemích třetího světa a současné bezpečnostní situaci, která se nemění k lepšímu (např. příklon k méně demokratické verzi Turecka a k rozvráceným mocenským uskupením v zemích třetího světa), je možné predikovat další zhoršení bezpečnostní situace.

Z tohoto porovnání je možné vyvodit závěr, že současné přijímané bezpečnostní opatření jsou oprávněná a je nutné se připravit i na moderní způsoby vedení asymetrického boje.

Z map teroristických aktivit získaných z portálu GTD (viz příloha 1 – obrázek č. 1 a č. 2) je však zřejmé, že hlavními ohnisky teroristických útoků není západní Evropa, avšak primárně země třetího světa, Afrika a oblast Čečenska.

Vliv na rozdíl mezi frekvencemi útoků v ohniscích dopadů teroristických útoků (země třetího světa, Afrika a oblast Čečenska) a mezi zeměmi západní Evropy má mnoho faktorů. Mezi faktory ovlivňující frekvence útoků patří vzdálenost od nestabilních zemí, systém vlády, stav a uspořádání společnosti, mezinárodní vztahy, náboženské prostředí a v neposlední řadě bezpečnostní systém.

Většinu z výše uvedených faktorů nelze jednoduchým způsobem v krátkém časovém rámci změnit, to však neplatí u poslední položky, tedy u bezpečnostního systému. Bezpečnostní systém lze adaptovat dle hrozeb, kterým musí daná společnost čelit. Jedním z důvodů, proč je západní Evropa v číslech obětí teroristických útoku na poměrně nízkých hodnotách, je mimo jiné právě adaptabilní bezpečnostní systém. Současný bezpečnostní systém je poměrně dobře připraven na konvenční hrozby, avšak je nutné provést další optimalizaci bezpečnostního systému díky novým hrozbám, které se v současné době vyvíjejí a to jsou kybernetické útoky a útoky dronů. Jejich vývoj a nárůst využívání bude znázorněn v následujících grafech.

5.2 Vývoj počtu kybernetických útoků a využívání bezpilotních letounů

V návaznosti na informace uvedené v předchozí kapitole budou uvedeny grafy, které znázorňují nárůst kybernetických útoků, která zaznamenal US-CERT. Nejdříve budou definovány týmy CERT a CSIR, neboť právě ty spolupracují i s americkou verzí CERT a poté uveden graf

vývoje kybernetických útoků. Následovat bude využívání grafické znárodnění využívání bezpilotních letounů k útokům.

CSIRT (Computer Security Incident Response Team) a CERT (Computer Emergency Response Team)

CSIRT a CERT jsou bezpečnostní týmy pro řešení bezpečnostních incidentů v rámci své působnosti – tedy informačních a komunikačních sítí - a jejich koordinaci. V České republice jsou zastoupeny týmem CSIRT.CZ A GovCERT.CZ. Jejich vznik započal v rámci ČR v roce 2007. V ČR spadají pod národní centrum kybernetické bezpečnosti (NCKB). [40]

Bezpečnostní tým CSIRT.CZ je provozován sdružením CZ.NIC, spravuje českou národní doménu, a to na základě veřejnoprávní smlouvy, která byla uzavřena v prosinci 2015 s Národním bezpečnostním úřadem, který je gestorem problematiky kybernetické bezpečnosti.

CSIRT.CZ má také ve své gesci předávání hlášení o bezpečnostních incidentech správcům domén a sítí, z kterých incidenty pocházejí, ale které jsou vůči stížnostem nereaktivní. Ve výsledku tedy v takových případech slouží jako jakýsi "institut poslední záchrany" pro případ, že alternativní metody kontaktování správců selžou. [41]

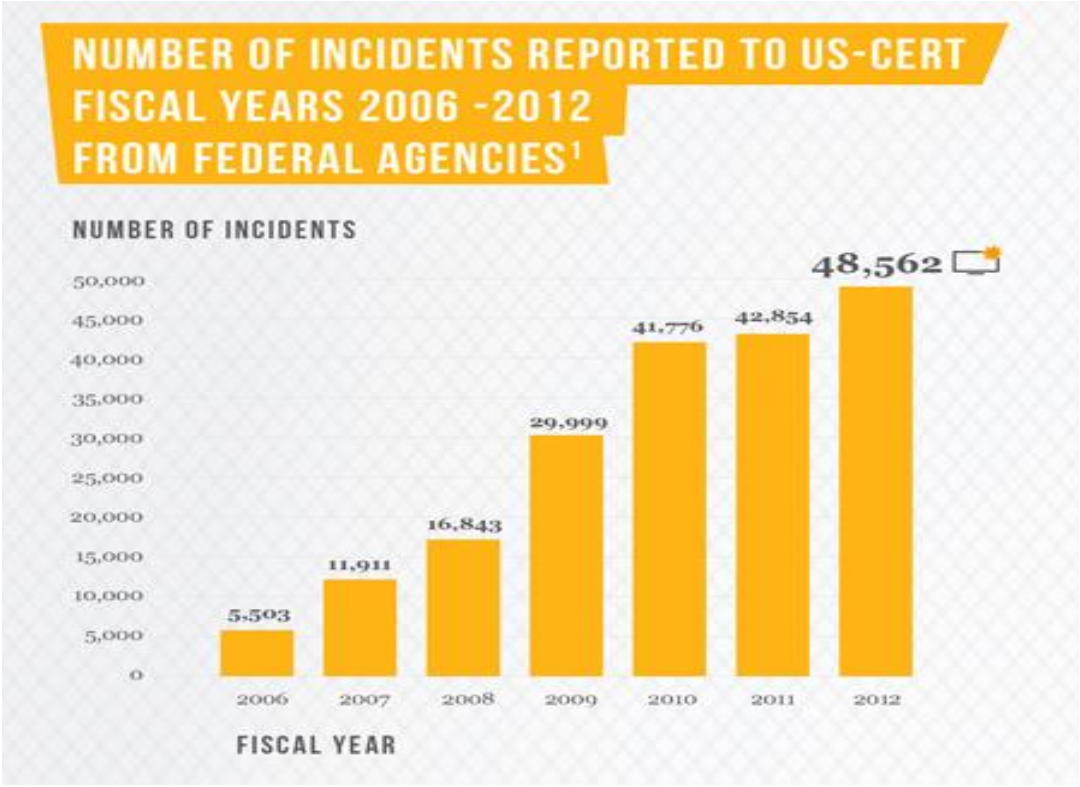
Úkolem CSIRT.CZ je poskytovat pomoc a rady poskytovatelům internetového připojení (ISP) v České republice a napomáhat zřizování jejich vlastních bezpečnostních týmů a bezpečnostní infrastruktury. Dále má za úkol řešit kybernetické bezpečnostní incidenty a ve výsledku zlepšovat bezpečnost internetových sítí i internetu globálně. [41]

Aktuálně je po celém světě oficiálně založeno přibližně 300 bezpečnostních týmů typu CERT/CSIRT. Ty jsou začleněny buď do organizace FIRST, anebo evropské platformy TF-CSIRT (popřípadě do obou).

V ČR je aktuálně oficiálně konstituováno a na globální infrastrukturu napojeno celkově pět bezpečnostních týmů typu CERT/CSIRT – dva z nich působí v rámci sítě národního výzkumu a vzdělávání - CESNET2 (týmy CESNET-CERTS a CSIRT-MU). Další provozuje sdružení CZ.NIC za účelem udržení dohledu nad sítí sdružení a DNS serverové domény .cz (CZ.NIC-CSIRT). Prozatím působí pouze jeden v privátním sektoru – tým Active24-CSIRT, který je provozován jedním z předních českých registrátorů (společnost Active24). Posledním týmem v tomto výčtu je výše zmíněný tým CSIRT.CZ. [42]

Na stránkách CSIRT.CZ se dále objevují aktuální zprávy o kybernetických hrozbách, útocích a odkazy, které navádějí, jak těmto útokům čelit a jak svůj systém zabezpečit – v době zpracovávání práce se jedná například o rozsáhlé útoky Ransomwaru (Ransomware je druh malware (škodlivý program), která slouží k zabránění přístupu k počítači, který je infikován za pomoci šifrování dat na disku. Tento program zpravidla požaduje po oběti zaplacení výkupného za zpřístupnění dat obsažených v počítači) WannCry. [41] [43]

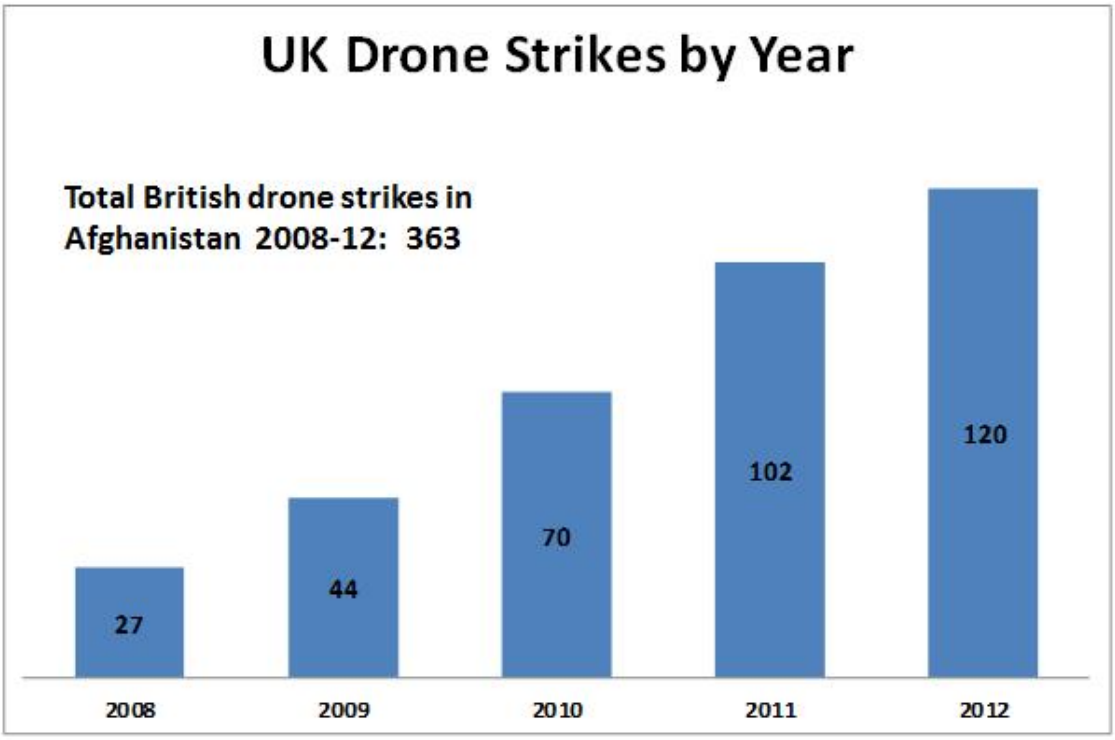
Z následujícího grafu vyplývá, že se počet kybernetických incidentů / útoků se neustále navyšuje, a proto je třeba adaptovat bezpečnostní systém, podporovat formování specializovaných týmů (viz. CSIRT a CERT) a rozvíjet mezinárodní spolupráci.



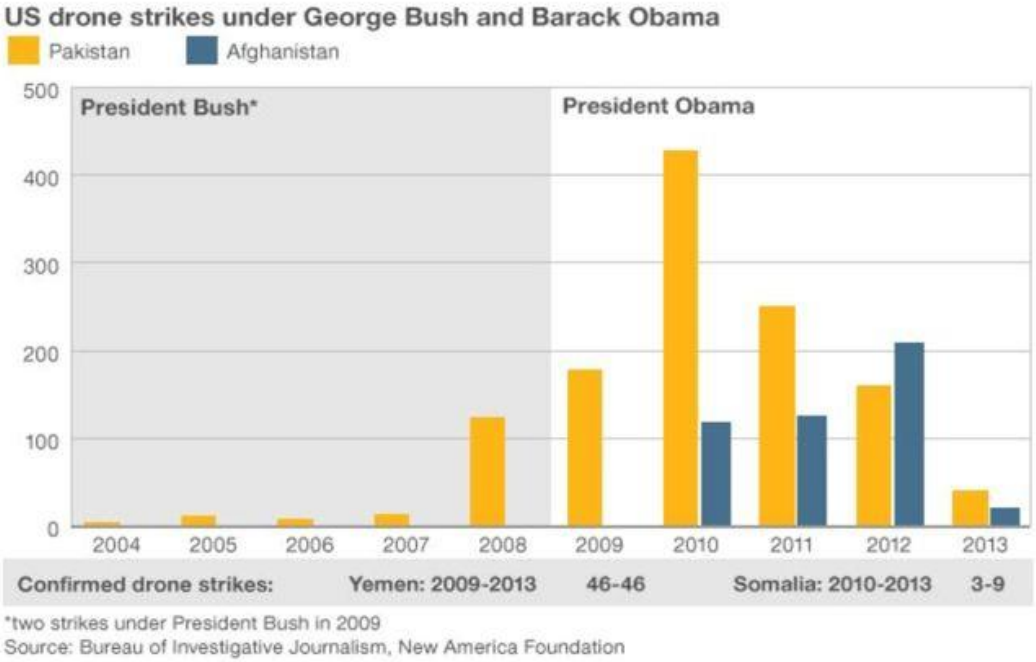
Graf 3 – Počet kybernetických incidentů zaznamenaných US-CERT (2006-2012) [44]

Z následujících grafu je zřejmé, že využívání bezpilotních letounů při vojenských akcích narůstá. V prvním grafu je znázorněn nárůst úderů za pomoci dronů mezi lety 2008 až 2012 na území Afgánistánu – jedná se takřka o exponenciální nárůst. Zástupci britské vlády tvrdí, že při útocích jsou minimální civilní ztráty a poskytuje záznamy z letu a útoku dronů ke zkoumání. Avšak ze samotných záznamů nelze zcela určit oprávněnost útoku, a zda zároveň s cílem nejsou zasaženi i civilisté. [45]

Druhý graf znázorňuje využití úderů bezpilotních letounů v průběhu různých administrativ v USA – tedy za doby úřadování prezidentů Bushe a Obamy. Barevně jsou rozlišeny útoky vedené na území Pákistánu (žlutě) a Afgánistánu (modře). Zde je možné vidět kolísání využití dronů, avšak v současné době je využití bezpilotních letounů znovu na vzestupu. Křivka v tomto případě kopíruje i vývoj konfliktu. [46]



Graf 4 – Počet úderů za využití dronů britskými silami v Afgánistánu (2008 - 2012) [45]



Graf 5 – Využití úderů dronů v Afgánistánu a Pákistánu během administrativy prezidentů Bushe a Obamy (2004 - 2013) [46]

Z předchozích grafů je zřejmé, že technologie a využívání bezpilotních letounů je na vzestupu, avšak není zřejmé, až do jaké míry se využití do budoucna zvýší. Určitou predikci poskytne následující výhledová graf, který předpovídá nárůst bezpilotních letounů (systémů) v letech 2015 – 2035.

Černou barvou je zobrazen celkový počet letounů držených veřejností (včetně ministerstva obrany) na území USA a modrou barvou počet dronů využívaných komerčně. Závěr je tedy takový, že do budoucna se bude muset problematika ochrany před drony řešit stále více. Predikce vychází z dat získaných ze statistik ministerstva dopravy USA. [47]

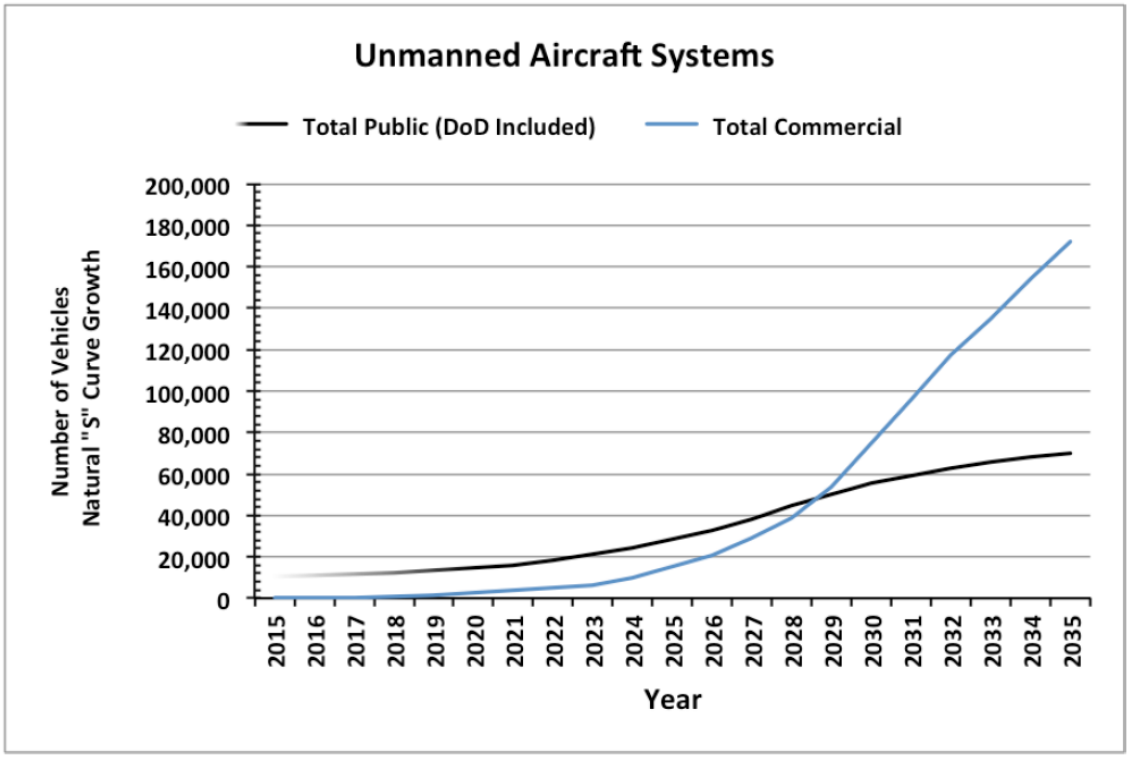


Figure ES-3 - Total UAS Forecast 2015 - 2035

Graf 6 – Predikce nárůstu využívání bezpilotních letounů (systémů) (2015 – 2035) [47]

5.3 Případové studie - nejvýznamnější kybernetické útoky, jejich viníci a následky

V následující podkapitole budou zmíněny některé z hlavních kybernetických útoků, které byly v posledních letech odhaleny. Právě otázka odhalení a publikování těchto útoků je v rámci kybernetických útoků a jejich zkoumání zásadní. Některé kybernetické operace probíhaly bez povšimnutí dlouhou řadu let, než byly odhaleny. Níže budou tedy zmíněny ty, které se odhalit podařilo. Každé zkoumání má rozsah stručné případové s následující strukturou – Název útoku, průběh útoku, jeho následky a předpokládaného viníka.

Aurora (2010)

Tento incident mnozí považují za historický milník, kde opravdu započal současný věk kybernetických zbraní (autor již výše uvádí dříve datovaný útok na Estonsko v roce 2007, avšak výše zmíněný útok nebyl v porovnání s tímto natolik sofistikovaný a nevěnovala se mu dostatečná pozornost), alespoň co se jejich zveřejňování v médiích se týká. Útok označovaný jako Aurora zasáhl napadenou zemi (USA) poměrně nepřipravenou. Čínští hackeři (alespoň jim je tento útok připisován) systematicky útočili na velký počet amerických organizací, včetně gigantických společností jako je Google, která nakonec útoky zveřejnila. Až doposud byly kybernetické útoky vnímány jako něco, co se děje zřídka kdy a směřují pouze na vybrané skupiny – toto vnímání Aurora změnila. Ve výsledku se nejednalo o komplexní útok, ale překvapivý a rozsáhlý. Americká ministryně zahraničí Hillary Clinton vydala veřejné prohlášení, v němž označila Čínu jako útočníka, což bylo poprvé, kdy jeden národ veřejně obvinil druhý národ za kybernetický útok. [48]

Důsledky útoku: Zvýšení vnímání hrozby kybernetických útoků, tvorba specializovaných jednotek k boji proti kybernetickým hrozbám, zařazení boje proti kybernetickým útokům do politických programů a rozvoj úpravy kybernetických útoků v mezinárodním právu.

Označený viník: Čína

Stuxnet (2010)

Stuxnet je pravděpodobně nejznámější kybernetický útok v historii, neboť je jeden z prvních, které byl důkladně zdokumentován. Stuxnet byl bezpečnostní orgány odhalen v roce 2010, avšak již po napáchání škod. Bezpečnostní experti se s takovým útokem setkali poprvé. Stuxnet byl poměrně sofistikovaný útok a jeho cílem byly průmyslové systémy SCADA, Stuxnet využil čtyři různé zero-day útoky (zero-day útok je ve svém jádru využití chyby systému, která ještě nebyla dříve využita a tedy následovně nalezena a opravena. Je to velká neznámá, která může být zneužita dříve, než experti a jejich software odhalí chybu v softwaru nebo hardwaru. Ve skutečnosti, zero-day útok nezanechává příležitost pro detekci před jeho spuštěním) [49] a navíc obsahoval neobvyklé prvky pro tento typ útoku, například vlastnosti útoku za pomocí červa (WORM), jako je možnost šířit se po USB discích. Ohnisko útoků bylo identifikováno v Iránu. Stuxnet dokázal, zjednodušeně řečeno, zahltit určitá tepelná čidla v jaderných zařízeních a tím je vyřadit z provozu, tím pádem způsobit ztráty a zpomalit vývoj jaderného programu v Íránu. Zpočátku nikoho nenapadlo, že by USA mohlo za tímto útokem stát, avšak později při podrobném zkoumání původu útoku a s přihlédnutím k sofistikovanosti útoku, nebyl nakonec pochyb. [48]

Důsledky útoku: možnost studie chování sofistikovaného útoku v praxi, zvýšení zabezpečení jaderných zařízení, uvědomění si možnost rozvíjení schopností útočného softwaru

Označený viník: USA a Izrael.

Red October (2012)

V rámci své dlouhodobé kampaně, kterou cílila Ruská federace na východní Evropu, kybernetický útok zvaný Red October zdůraznil, že státem koordinované kybernetické útoky nemusí být vždy stejné nebo se stejným zaměřením – jejich cíle byli rozdílné od výše uvedených útoků vedených USA. Útok Red October byl konstruován tak, aby vykonával „dohled" na diplomaty a vědci – tedy klasická novodobá špionáž – zachycení e-mailů, osobních zpráv, citlivých osobních dat atd. Útok byl poprvé zachycen bezpečnostní firmou Kaspersky Lab, která je sama ruského původu se sídlem v Moskvě, což vedlo k pochybám, jestli útoky pochází z Ruska, avšak ve výsledku to vedlo k domněnkám o nejednotnosti vlády. [48]

Důsledky útoku: Zvýšení zabezpečení komunikace mezi diplomaty a vědci**, podpora** nezávislých bezpečnostních firem v boji proti kybernetickým útokům

Označený viník: Rusko, Izrael

Shamoon (2012)

Před tímto útokem byly kybernetické útoky vnímány odborníky jako, nenápadné programy, které získávaly informace, či prováděli svoji činnost skrytě. Shamoon (také známý jako "Disttrack") tento pohled změnil. Shamoon měl za úkol ničit a podařilo se mu destruktivně zasáhnout saúdský ropný

průmysl v srpnu 2012. Poškozeno bylo více než 30 000 počítačů, které patřily saúdské ropné společnosti Aramco. Skupina útočníků, která se nazývá "Sekající meč spravedlnosti" (Cutting Sword of Justice), se k útoku přihlásila, což není v dnešní době typické, avšak díky nižší sofistikovanosti útoku a s ohledem na zemi původu je to pochopitelné. Tento útok byl prohlášen a publikován jako první útok, který měl čistě destruktivní účely. [48]

Důsledky útoku: Záplaty v systémech, úprava ICT infrastruktury, tvorba interních systémů pro minimalizaci rizika

Označený viník: Írán

Equation Group (2014)

Jeden z posledních objevených majoritních útoků se zdá být prozatím jeden z největších, útok Equation Group poukazuje na fakt, že se kybernetické útoky povznesly nad úroveň jedince a zdůrazňuje důležitost práce v týmu a to jak při jeho plánování, tak při jeho odhalování a neutralizaci. Útok Equation Group disponuje několika zajímavými schopnostmi, například schopností infikovat firmware pevných disků, což je dodnes nezmapovaná oblast – de facto útočníci dokázali přepsat část disku, na kterou by se nemělo zapisovat nic jiného, než základní data, které ovládají disk. V tomto případě ani formátování disků, které většinu malwaru odstraní, není účinné. [48]

Důsledky útoku: zkoumání využitelnosti a možnosti zneužití základních komponentů počítačů

Označený viník: USA

Za zmínku stojí další i další závažné útoky jako jsou:

- Sony Pictures Attack (2014) – útok na společnost z důvodu publikování kontroverzní komedie o vůdci Severní Koreje
- Darkhotel (2014) – sledování pohybu a získávání citlivých dat od top managementu nadnárodních korporací
- Regin (2014) – dlouhodobé sledování (počátek již v roce 2000) nepřátel, avšak i spojenců USA a UK – odhaleno v souvislosti s unikem informací od E. Snowdena (E. Snowden je bývalý systémový administrátor pracující pro americkou Národní bezpečnostní agenturu (NSA) a zaměstnanec CIA, který do tisku vynesl informace o masivním a do té chvíle před veřejností utajovaném celosvětovém sledování telefonů a elektronické komunikace ze strany bezpečnostních služeb USA.)

Výčet útoků není taxativní, slouží k ilustraci zapojení mnoha stran do kybernetických útoků, stejně jako k poukázání na fakt, jak se od sebe útoky liší a jejich zvláštnosti.

5.4 Praktické doporučení pro zvýšení kybernetické bezpečnosti

Níže budou uvedeny doporučení, které vznikly z rozhovoru s odborníky, kteří jsou ve své působnosti zodpovědní za kybernetickou bezpečnost ve zkoumaných společnostech (SÚRAO a Letiště Praha a.s.). Tyto poznatky vycházejí z analýzy každodenní činnosti a identifikují základní problémy bezpečnosti ve společnostech, avšak při zobecnění se dají tyto doporučení aplikovat na jakoukoli společnost nebo stát.

Problémy budou označeny a budou k nim přiřazena částečná řešení, která budou komplexně, společně s dalšími doporučeními, shrnuta dále v návrhách opatření.

- **Nedokonale nastavená uživatelská práva (chyba lidského faktoru)**

Pomocí správného nastavení uživatelských oprávnění a odebráním administrátorských práv, IT oddělení de facto chrání uživatele před sebou samým. Pomocí UAC (User Account Control - „Řízení uživatelských účtů“ – nástroj k nastavení přístupu uživatele k souborům a funkcím systému (spouštění programů apod.) dokáží správci systému přesně určit, jaký uživatel bude mít k čemu přístup, omezí se pak riziko napadení systému přes zavirované e-maily či přes flash disky – uživatel bez práv pak nemůže rizikový soubor (často s příponou .exe či .bat) spustit. Tento problém se vyskytl i na ve zkoumaných společnostech a zaměstnanci byli poučení, aby cizí flash disky do stanic nevkládali. Zároveň UAC nesmí být přehnaně restriktivní, aby pracovníka neomezoval v práci – optimalizací tohoto rozhraní se dosahuje bezpečnějšího kybernetického prostředí v rámci společnosti i při komunikaci s vnějším světem.

Příkladem špatného UAC (který vyšel z diskuze s IT pracovníkem společnosti) je výše uvedený útok Stuxnet z roku 2010, který se mimo jiné přes e-maily zaměstnanců dostal do systému a vedl k napadení jaderného zařízení přes protokoly SCADA, kde upravil teplotní čidla (jejich treshold – mezní hodnotu), čidlo nehlásilo přehřátí a došlo k odstavení reaktoru. Dalším doporučením, které sníží riziko chyby lidského faktoru je varování zaměstnanců, aby nevkládali cizí přenosné disky do pracovních počítačů (flash disky, CD, DVD…), existují například flash disky (BAD USB), které dokážou po připojení vyvinout elektronický výboj o velikosti 2000V, které počítač naprosto vyřadí.

- **Málo rozvinutá komunikace mezi zaměstnanci a IT oddělením**

Častým problémem je absence efektivní a včasné kontaktování IT oddělení ve společnosti při výskytu jakéhokoliv kybernetického problému. Zaměstnanci často ze strachu z postihu, když učiní chybu a umožní viru proniknout do systému, raději informaci zamlčí. Čím větší společnost, tím je většinou ve společnosti určitá anonymita a lidé spoléhají na to, že si problému nikdo nevšimne nebo odezní. Opak je pravdou. Čím dříve se útok odhalí, tím rychleji mohou odpovědní lidé problém napravit a učinit opatření.

Jak s tímto problémem bojovat? Jak rozvíjet a motivovat ke komunikaci s IT oddělením? Pracovníci zaměstnaní v IT sektoru jsou často vnímáni jako velice specifičtí lidé (jiný dress code apod.) a tak je potřeba, aby si zaměstnanci zvykli s nimi komunikovat běžným způsobem a aby tato komunikace byla obousměrná. Dalším způsoby jsou:

- Zvyšování IT gramatiky zaměstnanců za pomoci školení (Nejlépe s osobním setkáním, nikoliv pouze e-formou, která je vysoce neosobní, i když zcela jistě levnější).
- Odstranění stigmatu, že nahlášení problémů či útoku může poškodit kariéru zaměstnance – naopak určitým způsobem odměnit nahlášení problému (např. darováním licence na některý program).
- Ochrana zaměstnanců i u nich doma – často útočníci využívají i domácí sítě zaměstnanců, aby se pak zprostředkovaně dostali do sítě v zaměstnání (napadení přenosných zařízení, emailů apod.).
- Konstrukce a implementace programů pro zvýšení bezpečnosti – častá změna hesel, která musí být zaměstnancům vysvětlena (Microsoft doporučuje měnit hesla v sítí každé 3 měsíce).

- **Kvalitní antivirové řešení a monitoring konečných stanic**

Nehledě na zabezpečení sítě je potřeba vždy na konečné stanici mít nainstalovaný antivirový program, což jedna ze zkoumaných společností nedodržuje. I když kontrola sítě zvenčí může být dobře řešena, při absenci antiviru se síť vystavuje riziku útoku zevnitř (viz. lidský faktor výše). Dalším problémem je, že lidé často opouštějí své stanoviště a neodhlašují se ze systému, i když u počítače nejsou. Tím se otevírá možnost vzdáleně ovládat počítač útočníky (přes vzdálenou plochu – např. pomocí Teamviewru). Tyto útočníci mohou například přes kamerový systém monitorovat, zda je stanice opuštěna a v tu dobu podniknout útok bez rušení. Jaké je řešení? Nastavit automatické odhlášení z počítače při nečinnosti, avšak to vždy zanechá určitě časové okno nebo poučit zaměstnance, aby se odhlašovali – stačí zkratka Win (Klávesnice s ikonou Windows (oknem)+L. Dalším problémem jsou útoky přes herní portály, řešení je jednoduché - zakázat nebo povolit přístup jen vybraným zdrojům.

- **Kontrola externích firem, které spolupracují se společností**

Komunikace s „ důvěryhodným zdrojem“, za který jsou spolupracující externí firmy často považovány, musí procházet stejnými postupy, jako by se jednalo o firmu cizí, neboť IT oddělení společnosti nemá detailní povědomí o jejich bezpečnostním prostředí a jejich postupech. Nastavit tedy automatické skenování souborů u všech spolupracujících subjektů, automatické sbírání dat od všech subjektů a správně nastavit logování (de facto podrobné záznamy o každé akci, která byla v rámci sítě provedena) a jeho propojení v souvislosti s okamžitým využitím IT oddělením, což oddělení umožní okamžitou či pozdější kontrolu události.

- **Správné nastavení zpětné vazby (feedback)**

Nastavit správně politiku přijímání podnětů od zaměstnanců je velice důležité, aby nedošlo k zahlcení IT pracovníka a ve výsledku nevyšlo ke špatnému vyhodnocení hrozby. Určený IT pracovník musí dále nejen na základě zpětné vazby identifikovat slabá místa systému a navrhnout investování k posílení těchto slabých míst – ve výsledku usilovat o neustálou eliminaci zranitelných míst.

- **Ochrana serverů a citlivých míst**

Ochrana serveru by se nikdy neměla podceňovat, nelze spoléhat pouze na softwarové firewally, server musí být vždy za fyzickým firewallem nebo jak ho určití lidé označují „ kusem železa“, přes který může IT pracovník kontrolovat veškeré porty a jednotlivé aplikace, což mu dává možnost zvýšené ochrany před DDoS útoky, dokáže efektivněji identifikovat falešné pakety a zabránit tak zahlcení systému. Co se týče citlivých míst, tím autor myslí například nezabezpečené sítě Wi-Fi. Základem je takové sítě nezřizovat a nepřipojovat se k nim – tyto sítě jsou zranitelné vůči MitM (Man in the middle (Útok s prostředníkem) - podstatou útoku je snaha útočníka odposlouchávat komunikaci mezi účastníky tak, že se stane aktivním prostředníkem – v našem příkladu je tímto třetím aktivním prostředníkem nezabezpečená wi-fi.). I začátečník dokáže této zranitelnosti využít, před určitou dobou se dokonce dala získat zdarma oficiální aplikace, která tento útok umožnila přímo na obchodu Google. Avšak pouhým jednoduchým heslováním se stane konverzace mezi zařízeními těžko zachytitelná a hlavně rozluštitelná, při aplikaci WPA2 je to obtížné i pro velmi schopného útočníka – resp. zkušenější útočník by raději hledal jinou cestu. Ve výsledku je odposlouchávání v reálném čase nereálné.

(Pozn. Autora – síťové karty od společnosti Intel mají integrované čipy pojistku proti zneužití pro MitM útoky.)

- **Zapojení se do projektů ke zvýšení kybernetické bezpečnosti**

Příkladem může být Projekt Turris, který se soustředí na sbírání dat za pomoci „bezpečnějších" routerů vlastního designu, a při analýze dat se pokouší identifikovat atypické vzorce chování paketů a tím pádem odhalovat i útoky. V rámci zapojení routerů získají členové i technickou podporu týmu, který jim může v případě nouze pomoci. Mimo jiné IT oddělení společnosti může navázat vztahy s dalšími odborníky a prohloubit své znalosti.

- **Ochrana hardwaru a softwaru společnosti před vestavěnými prostředky k útoku**

Bohužel bývají útočníci stále více vynalézaví nebo recyklují „staré dobré" nápady na novou techniku. Řeč je o hardwaru a softwaru, který má v sobě zabudované programy třetí strany, které mohou získávat data, odposlouchávat komunikaci apod. – tyto zařízení mohou být např. klávesnice, mobilní aplikace nebo dokonce harddisky, které v uživateli nepřístupné části paměti uchovávají malware (harddisky viz útoky výše). Jak se těmto útokům bránit? Používat pouze ověřený a společností označený, zaevidovaný hardware a software, veškeré neautorizované výměny hlásit IT oddělení. Další možností, která není na straně uživatele, ale IT oddělení je zavedení funkce autorizace klávesnic a ostatního hardwaru – tuto funkci poskytuje například produkt Kaspersky end point Security. Bohužel tato služba je zatím ve vývojové fázi, je určena pouze pro firmy a vyskytují se v ní například problémy s konektivitou určitých zařízení (tablety a určité typy klávesnic – dokovatelné, multifunkční apod.)

5.5 Příklad kybernetických útoků – DROWN útoky

Jako příklad kybernetických útoků budou uvedeny DROWN útoky. DROWN (Decrypting RSA with Obsolete and Weakened eNcryption – dekripce RSA se zeslabeným šifrováním) útoky jsou vážnou a aktuální hrozbou, která ovlivňuje HTTPS (HTTPS (Hypertext Transfer Protocol Secure) je v informatice nadstavba síťového protokolu HTTP, která umožňuje zabezpečit spojení mezi klientem) a další služby, které spoléhají na protokoly SSL a TLS - tedy některé ze základních kryptografických protokolů pro zabezpečení ICT systémů a webového rozhraní. Tyto protokoly umožňují každému uživateli na internetu procházet web, používat e-mail, nakupovat on-line a posílat okamžité zprávy bez možnosti třetích stran zachytit a zneužít komunikace mezi dotčenými stranami Z důvodu jejich aktuálnosti a závažnosti se autor rozhodl jim věnovat samostatnou kapitolu, i když samozřejmě patří do skupiny kybernetických útoků, která je zpracovávaná výše.

DROWN útok umožňuje útočníkům prolomit šifrování výše zmíněných protokolů a zachytit, přečíst nebo ukrást data z citlivých komunikací, včetně hesel, čísel kreditních karet, obchodních tajemství či finančních údajů. Dle odborných odhadů je 33% všech serverů HTTPS náchylných k útoku.

Útočníci mohou ve výsledku získat jakákoli data o komunikaci mezi uživateli a serverem. Útočníci obvykle, avšak ne vždy, cílí své útoky k získání uživatelských jmen a hesel, čísel kreditních karet, e-mailů, rychlých zpráv (facebook, messenger…) a citlivých dokumentů. V některých situacích může útočník také vydávat své upravené stránky k získávání dat za zabezpečené webové stránky a odposlouchávat nebo měnit obsah stránek, které uživatel vidí. [71]

Kdo je ohrožen?

Ohroženy jsou webové stránky, e-mailové servery, další TLS-závislé služby a velké množství populárních internetových služeb (od taxi společností jako Uber, po informační systémy vysokých škol). Odborníci, kteří na problém upozornili a tvůrci stránky https://drownattack.com/ provedli skenování určitých „zabezpečených" stránek na internetu, aby identifikovali, kolik subjektů je ohroženo a níže je uveden výsledek (výsledek je rozdělen do skupin):

Tabulka 6 Zranitelnost domén vůči DROWN útokům [71, vlastní tvorba]

Typy zkoumaných a testovaných domén	***Procento zranitelných domén***
HTTPS - Top jeden milion domén	***25%***
HTTPS - všechny stránky prohlížeče důvěryhodné	***22%***
HTTPS - všechny stránky	***33%***

Moderní servery a klienti používají šifrovací protokol TLS (Transport layer security – protokol umožňující aplikacím komunikovat po síti způsobem, který zabraňuje odposlouchávání či falšování zpráv.

Nicméně, vzhledem k chybné konfiguraci, mnoho serverů také stále podporuje SSLv2 (Secure Sockets Layer – Vrstva bezpečných socketů - poskytuje zabezpečení komunikace šifrováním a autentizaci komunikujících stran – předchůdce TLS), předchůdce TLS z let 90-tých. Podpora SSL protokolu v praxi dříve nevadila, protože žádný moderní prohlížeč SSLv2 nepoužívá. I když SSLv2 známé tím, že špatně vysoce nezabezpečený, tak až donedávna nebyla podpora serverů protokolu SSLv2 považována za bezpečnostní problém, protože klienti ho zřídka kdy využívali.

DROWN útoky však ukázaly, že pouhá podpora SSLv2 je skutečnou hrozbou pro moderní servery a klienty. Protokol SSLv2 umožňuje útočníkovi dešifrování moderního šifrovaného spojení mezi moderním klientem a serverem vysláním sond k serveru, který podporuje SSLv2 a používá stejný soukromý klíč. [71]

Provozovatelé zranitelných serverů potřebují přijmout příslušná opatření. Není nic prakticky možné, aby vývojáři prohlížečů nebo koncoví uživatelé ovlivnit tuto zranitelnost samostatně – chyba je bohužel v systému. [71] [72]

Jak chránit servery před DROWN útoky?

Pro zajištění ochrany proti DROWN útokům musí provozovatelé serverů zajistit, aby jejich soukromé klíče nebyly používány se serverovým softwarem, který umožňuje SSLv2 připojení. To zahrnuje webové servery, servery SMTP (Simple Mail Transfer Protocol je internetový protokol určený pro přenos zpráv elektronické pošty (e-mailů) mezi přepravci elektronické pošty), IMAP (I*MAP (*Internet Message Access Protocol) je internetový protokol pro vzdálený přístup k e-mailové schránce prostřednictvím e-mailového klienta) a POP

(*POP* (Post Office Protocol) je internetový protokol, který se používá pro stahování emailových zpráv ze vzdáleného serveru na klienta) serverů a jakýkoli jiný software, který podporuje TLS/SSL.

Vypnutí protokolu SSLv2 je řešením k odstranění bezpečnostní hrozby, avšak u některých serverů, může být složité a závisí na konkrétním softwaru serveru. Zkoumání způsobů vypínání výše uvedeného protokolu je však nad rámec této práce a vyžaduje pokročilejší znalosti ICT, z tohoto důvodu zde autor uvede odkazy na stránky, kde by čtenář mohl dohledat návody k vyřešení problému s tímto protokolem (jeho inhibice či smazání) - https://drownattack.com/ (AJ), kde se nachází více typů návodů na různé softwary a např. https://csirt.cz/ (CZ), zde se nachází návod k testování zranitelnosti a návod na vypnutí protokolu, avšak zde není zohledněn rozmanitý software serverů [71]

Samozřejmě existuje více typů útoků a dalších metod, které se dají ke kybernetickému útoku použít a samozřejmě i více způsobů, jak tento útok či původce skrývat, avšak výše uvedené jsou v dnešním světě používané nejvíce a v minulosti zasáhli různé evropské státy i ČR.

5.6 Ochrana objektů před bezpilotními letouny

V následující kapitole bude v rámci koncepčního projektu zhodnocen aktuální stav ochrany objektu (Letiště Praha a.s.) vůči útokům bezpilotních letounů a navrhnuty různé způsoby řešení ochrany objektu výše zmíněným útokům.

5.6.1 Současný stav ochrany objektů před bezpilotními letouny

V současné době je ve zkoumané společnosti ochrana před bezpilotními letouny řešena neoptimálně. Zjištění letounu je zajištěno pouze vizuálním

způsobem či v některých případem perimetrickým radarem, který však není pro takovou detekci uzpůsoben. Každý člen ozbrojených složek dostal v rámci školení pokyn eliminovat bezpilotní letoun palnou zbraní za podmínky, že bezpilotní letou ohrožuje chráněné zájmy v oblasti civilního letectví a v okolí se nenachází žádná osoba, která by mohla přijít k újmě na zdraví a zároveň by nezpůsobil škodu na jednotku, bezpilotní letou vyjímaje. Tento stav není optimální, a proto se v současné době hledají alternativní řešení. Avšak technologie pro detekci a eliminaci dronů, které jsou vhodné pro civilní užití a jsou finančně dostupné, se stále vyvíjí, proto budou v následující části představeny koncepce pro řešení daného problému.

5.6.2 Současná koncepce možné budoucí ochrany před bezpilotními letouny

V plánu investic společnosti je obsažen záměr vybudování detekčního systému bezpilotních letounů. V prvotní fázi je nutné určit, proti jakým typům bezpilotních letounů jsou různé typy ochran účinné a jakou formou. U uvedených způsobů budou vždy posouzeny okolnosti použití systému a jejich vhodnost.

Zkoumaný objekt je objektem civilním, což zužuje výběr systému ochrany, neboť nemůže např. využívat raketovou obranu, jako objekty vojenské.

Pokud by tomu tak nebylo, bylo by možné využít např. raketové systémy Pečora 2M, které v současné době operují například na území Sýrie. Ty dokázali v dubnu 2017 (22.4.2017 17.40 hod. GTM) sestřelit americký bezpilotní letou Predator MQ-1. Sestřelení drona proběhlo nad základnou Šajrát, samotný dron startoval ze základny Incirlik, kde americká armáda uchovává větší množství dronů typu Predator. Podle zpráv plnil sestřelený letoun bojový úkol.

Ve výzbroji syrské armády je v současné době 12 systémů Pečora 2M, které jsou značně mobilní (dokáží se pohybovat rychlostí až 60 km/h) a dokážou se tak přemístit v rámci prevence proti cíleným odvetným útokům. Navíc disponují i technologií k odhalování „stealth“ (skrytých) letounů a následně je mohou sestřelit. Avšak i v takovém počtu (12 raketových systémů) nedokážou raketové systémy pokrýt celé území Sýrie. [50]

Využití takového systému, proti dronům bojového typu je odůvodněné, neboť cena rakety i dronu je přibližně srovnatelná – naopak je v tomto případě cena rakety nižší než konstrukce dronu. V následujícím odstavci však bude (částečně v rámci drobné recese) uveden i opačný přístup, který znázorní, že finanční stránka věci nemusí hrát vždy roli.

Spojenci USA využili na sestřelení běžného drona (tedy nikoliv dron typu predator či reaper (modernější verze predatoru)) v ceně pohybující se kolem 300 eura raketu z platformy patriot, která sice dron efektivně eliminovala, avšak cena opatření je v naprostém nepoměru. Na dron v ceně pohybující se v cenové relaci 300 eur byla vypálena raketa, jejíž cena je 3 miliony dolarů. Tato raketa dokáže pětinásobně přesáhnout rychlost vzduchu a dokáže v určité konfiguraci chránit před balistickými střelami, které mohou nést jaderné hlavice. Generál David Perkins, který obranu spojenců zaštitoval, se k incidentu odmítl oficiálně vyjádřit, avšak na pořízené fotografii z útoku poukazuje na destrukci dronu v letu a usmívá se. Při tiskové konferenci k incidentu se přítomní armádní experti vyjadřovali ve smyslu, že americká armáda je vybavená nejlepším (a tedy i jedním z nejdražších) vybavením a že jejich nepřátelé využívají civilní prostředky, které jsou ve výrazném cenovém nepoměru. [51]

Za zamyšlení občas stojí reálný nepoměr vynaložených prostředků na eliminaci bezpilotního letounu. Z tohoto a výše uvedených důvodů (např. nemožnost využití v civilní sféře) je nutné raketové systémy z možnosti ochrany zkoumaného objektu vyloučit, avšak s určitým důrazem na cenovou redukci je toto řešení vhodné pro objekty vojenské. Výhoda systému je takové, že dokáže bezpilotní letoun eliminovat takřka bez ohledu na typ – není třeba spoléhat na inhibici spojení mezi pilotem a dronem (nemožnost využití u autonomních letounů) a je možné zasáhnout i letouny pohybující se značnou rychlostí.

Dále bude zmíněno řešení, které se aktuálně připravuje pro zkoumaný objekt, a následovat budou alternativní řešení, z nichž by se některé mohli k současně navrhovanému systému připojit.

V rámci zkoumaného objektu je aktuálně připravován projekt, který se soustředí na první fázi ochrany před bezpilotními letouny – tj. jejich identifikace v chráněném prostoru. Pro tento záměr je zvažována jako dodavatel společnost R&S a jejich produktová řada ARDRONIS.

Systém R&S ARDRONIS je řešením automatické identifikace rádiem ovládaných dronů a je řešením pro náročné aplikace sledování dronů. Zároveň se specializuje na vytváření protiopatření proti bezpilotním letounům. Má široké rozmezí užití proti různým typům dronů – od mikrodronů po letouny větších rozměrů. Specializuje se na dálkově ovládané drony a úkolem ochrany je primárně navést ozbrojené složky k místu ovládání drona. Systém poskytuje funkce určené k včasnému varování a k rychlé detekci bezpilotních letounů. Drony dokáže identifikovat v časovém rámci, kdy je zapnut dálkový ovladač dronu – tedy ještě před startem dronu. Pomocí triangulace signálu dokáže určit směr navedení k obsluze dronu a dokáže rušit signál. Funguje na principu

sledování radiokomunikačních linek, spolehlivě detekuje specifické signály dálkového ovládání, zjisti směr, z kterého je dron ovládán a zahájí systém přerušení komunikace. Systém má funkcionalitu vymezení chráněné oblasti, což je užitečné k eliminaci falešných poplachů, zvlášť vzhledem k tomu, že zkoumaný objekt je letiště a tedy se ve vzduchu nachází neustále velké množností objektů. Veškeré ovládání je integrované do jediné platformy a má upravitelné uživatelské prostředí. Systém dokáže dále klonovat přenos videa tím pádem replikovat přenášený obraz operátorům systému ARDRONIS. Pro různé uživatelé je možné dosáhnout různého stupně optimalizace, který je popsán v následující tabulce. [52]

Tabulka 7 Funkcionalita různých řešení systémů ochrany před drony [52, vlastní tvorba]

Balíčky řešení	*Dostupné funkce*		
	Identifikace	Zaměření	Protiopatření
R&S ADRONIS-I Detection	**x**	-	-
R&S ADRONIS-D Direction	x	x	-
R&S ADRONIS-R Disruption	x	-	x
R&S ADRONIS-P Protection	x	x	x

Na základě výše uvedené tabulky je možné zvážit vhodné řešení pro různé objekty a zohlednit jejich potřeby a finanční možnosti, neboť systém s více funkcemi potřebují více komponentů a jejich pořízení je různě finančně náročné. Označením [X] je znázorněna dostupnost funkce u každého řešení a označením [–] je naopak jeho nedostupnost.

Jak již bylo zdůrazněno na začátku podkapitoly, ochrana proti bezpilotním letounům je stále ve vývoji a v následující tabulce bude znázorněna

dokončenost / datum dokončení jednotlivých verzí systému – označení Q znamená kvartál dokončení. V rámci zkoumaného objektu bude prozatímně instalován systém R&S ADRONIS-D Direction do doby, dokud nebude dostupný systém se všemi funkcionalitami.

Tabulka 8 Dostupnost různých řešení systémů ochrany před drony [52, vlastní tvorba]

Označení systému	*Typ systému*	*Dostupnost / plánovaná dostupnost*
R&S ADRONIS Detection	R&S ADRONIS-I	3Q 2016 - dokončeno
R&S ADRONIS Direction	R&S ADRONIS-D	4Q 2016 - dokončeno
R&S ADRONIS Disruption	R&S ADRONIS-R	2Q 2017 – ve vývoji
R&S ADRONIS Protection	R&S ADRONIS-P	3Q 2017 – ve vývoji

Specifikace jednotlivých systémů včetně komponentů je znázorněna dle jednotlivých řešení v příloze č. 2.

5.6.3 Alternativní a možná souběžná řešení ochrany objektu před bezpilotními letouny

Jako alternativy či možná souběžná řešení budou níže uvedeny další způsoby řešení ochrany před bezpilotní letouny.

Již v úvodní části kapitoly byl zmíněn současný stav ochrany zmíněného objektu, který je v současnosti neoptimální. Palba ostrou municí na létající dron v zastavené oblasti a tím zvláště v prostorách letiště, kde jsou zájmové objekty, i ve vzduchu není optimální. Tento zákrok může způsobit více škody než užitku a zvlášť za současného stavu, kdy jsou k „sestřelování“ bezpilotních letounů

instruovány nespecializované ozbrojené složky, které nemají specializované zbraně k tomuto účelu.

Jednou z cest je sice také projektilová ochrana, ale neletálního charakteru. Touto cestou je metání sítí vůči bezpilotnímu letounu. Toto řešení poskytuje např. britská společnost Skywall. Ta za pomocí rakety a přenosné ruční platformy poskytuje možnost fyzicky zachytit bezpilotní letoun do speciální sítě. Tento systém byl například využit k ochraně amerického prezidenta při návštěvě v Berlíně. Jejich platforma s názvem SKYWALL 100 je přizpůsobena pro palbu mnoha typu projektilů – za zmínku stojí právě zmiňované sítě proti dronům dvojího typu (přímá střela a střela s padákovitým dopadem), tréninkové projektily, konvenční střely ráže 40mm a 81 mm či dokonce pracují na projektilu, který dokáže vyvolat elektromagnetický puls, který zničí elektronické zařízení. Platforma je dále vybavena adaptabilním systémem zaměřování, který usnadní zasáhnutí cíle a díky tomuto zaměřování není potřeba dlouhého tréninku na přesnost. Další výhodou je ekonomická nenáročnost, neboť pořizovací cena je oproti ostatním obdobným systémům nižší a projektily se dají recyklovat a znovu použít. Zároveň je zde jednoduchá možnost rozšíření ochrany pouhým přikoupením dalších platforem při eskalování rizika útoku dronů. [53] [54]

Výhodou tohoto zařízení je přenosnost, neletální charakter při využití sítě, možnost tréninku ozbrojených složek, recyklovatelnost a připravenost na další vývoj efektivních projektilů vůči hrozbám.

Nevýhodou je omezené užití vůči vojenským dronům, zhoršená schopnost zasáhnout rychle se pohybující cíl, nutnost dostat se na poměrně malou vzdálenost k cíli. Ve výsledku bych doporučil tento systém ochrany zvážit a doplnit k systému detekce, zvlášť díky poměru výkon / cena.

Dalším alternativním způsobem je metoda bojování „ohněm proti ohni“. Tedy využít k eliminaci dronu dalšího drona. V uplynulém roce zažil průnik dronu do střežené oblasti Bílý dům, premiér Japonska a kancléřka Merkelová. Dron použitý k eliminaci útočícího drona musí být ve výsledku lepší – rychlejší, obratnější a lépe vyzbrojený.

Inženýr z MIT (Massachusettského technologického institutu) vyvinul takový typ bezpilotního letounu, který nazval Falcon (sokol) a ten je schopný v letu zablokoval útočící dron, vypálit na něj síť nebo do útočícího drona narazit a způsobit explozi, která sice zničí oba drony, ale eliminuje riziko. [53] [55]

Toto řešení je sice zajímavé a rozhodně by přitáhlo mediální pozornost, není finančně náročně a jistě by přineslo i určitou formu oživení pro bezpečnostní složky ve zkoumané společnosti, avšak v této formě bych tuto formu ochrany nedoporučoval. Drony by bylo vhodné využít v rámci zkoumané společnosti pro hlídkovou činnost v semi-autonomním režimu. Dron by měl naplánovanou trasu dle GPS souřadnic, která by nešla bez potvrzení fyzickým tokenem změnit (prevence proti převzetí kontroly nad dronem třetí osobou) a operátor by měl možnost drona zastavit, donutit k přistání (v případě naléhavé situace) a ovládat záznamové zařízení (video, audio).

Alternativou k výše uvedeným fyzickým způsobům zajištění je určitý systém prevence. Společnost DJI (Da-Jiang Innovations Science and Technology), gigant v oblasti prodeje a vývoje bezpilotních letounů, do svých dronů nechává kompulzivně zabudovávat GPS lokátor, který snímá polohu letounu, což je dobré pro pilota letounu, avšak dá se využít i k restrikci letového prostoru. Pokud se dron dostane do blízkosti např. mezinárodních letišť nebo vojenských základen, které se do projektu zapojí, pak narazí na bariéru, která mu znemožní dál pokračovat v letu daným směrem. Ochrana samozřejmě není

absolutní a při úpravě dronu zručným „hackerem“ se dá obejít, avšak tento krok znatelně redukuje počet potenciálních incidentů s amatérskými uživateli, kteří nemají v úmyslu někoho zranit, avšak pouze chtějí ukojit svou zvědavost nebo pořídit unikátní záběry. Názornou ukázku prostředí takového ovládání na základě restrikce za pomoci GPS lze nalézt v příloze č. 3. [53] [56]

Dalším způsobem řešení (nápad, který má sympatie autora) je využití vzdušných prostředků, které dominovali vzdušnému prostoru dlouho před námi a to jsou ptáci, přesněji dravci. Dravci dokážou vyvinout při střemhlavém letu neuvěřitelné rychlosti, jsou přesní, dokáží eliminovat hrozbu efektivně a v letištním prostředí mají více využití. V rámci zkoumané společnosti je konstituována jednotka BOL (biologická ochrana letiště), která má k dispozici několik dravců, kteří by při vhodném výcviku mohli tento úkol převzít a poskytnout tak další možnost ochrany prostorů zkoumané společnosti před bezpilotními letouny. Společnost nabízí možnost zakoupení již trénovaného dravce, možnost vytrénování dravců, které si zákazník dodá (ten by se dal využít ve zkoumaném případě) a dále nabízí výcvik ptáčníků či výcvik ostrahy takovým způsobem, aby dravce uměl ovládat. [53]

Výhody výše zmíněného způsobu jsou ekonomická nenáročnost (Letiště Praha a.s. disponuje vlastními dravci a ptáčníky), krátká doba výcviku / zhotovení opatření a mediální pozornost, která je se zavedením spojená. Jako jedinou nevýhodu spatřuji v lidském popř. „zvířecím“ faktoru. Akce zvířat jsou stejně jako u lidí často nepředpověditelné.

K této metodě bude připojeno další doporučení a to je využití výše zmíněny jednotky BOL jako alternativu k „sestřelování“ bezpilotních letounů nespecializovanými složkami. Jednotka BOL je vybavena dlouhými zbraněmi,

které jsou uzpůsobeny ke střelbě ptactva, tedy jsou nejbližším možným řešením eliminace bezpilotních letounů za pomoci konvenčních palných zbraní

Posledním systémem, který zde bude zmíněn je pouze jistá variace na systém zmíněný v úvodu podkapitoly – tj. R&S ARDRONIS. Jedná se o variaci tohoto systému od jiného výrobce – britské společnosti Blighter. Svůj systém nazvala AUDS (Anti-UAV Defence System). Funguje obdobně jako jedna z variant systému ARDRONIS, zamíří se na cíl a obsadí se všechny ovládací frekvence a dron je ve vzduchu inhibovaný. [57]

Výhodou tohoto systému je přenosnost, kdy přenosný kufřík váží přibližně 25 kg a jeho cena je přibližně 300 tisíc korun. Nevýhodou je omezený dosah, který je přibližně v okruhu 2 km. Při nižší ceně dokáže systém od R&S pokrýt celou plochu letiště. Společnost Blighter samozřejmě nabízí i výkonnější soustavy, avšak ty jsou v naprosto jiné cenové relaci (řády jednotek až desítek milionů korun). Navíc v současnosti ve zkoumané společnosti již jedno zařízení od společnosti Blighter působí a zkušenosti s ním nejsou zcela kladné. [57]

6 DISKUZE

V rámci diskuze budou shrnuty hlavní myšlenky a přínosy práce, názory dalších autorů na související témata, bude vyhodnoceno potvrzení hypotéz.

V rámci teoretické i praktické části byli uvedené různé pokusy o definici fenoménu terorismus. Byli citováni různí autoři a instituce, které se danou problematikou zabývají. Autor se ztotožňuje s v uvedené řadě s poslední definicí, která je uvedena v teoretické části a ta zní: *„Terorismus znamená cílevědomé použití násilí páchaného vládními agenty nebo subnárodními skupinami, obvykle proti nebojujícím osobám, za účelem získání pozornosti veřejnosti a jejího následného ovlivňování. V nejobecnější rovině je však terorismus chápán jako forma organizovaného násilí, obvykle záměrného proti nezúčastněným osobám, za účelem dosažení politických, kriminálních a jiných cílů.“* [5, s. 8].

Různí autoři definují ve svých monografiích terorismus různým způsobem a těžko lze označit některý za špatný, pokud splňuje základní podmínky a ty jsou definovány metodou provádění násilí, cílem a úmyslem. Pro ilustraci lze uvést autora monografie The Staircase to Terrorism, Fathaliho Moghaddama, který definuje terorismus následovně: *„Terorismus je politicky motivované násilí, páchané jednotlivci, skupinami nebo státy, s úmyslem roznítit v populaci pocity strachu a bezmoci za účelem ovlivnit procesy rozhodování a změnit chování.“* [58]

I když název práce zní: „Terorismus jako významná bezpečnostní hrozba“, není podstatná část věnována definici fenoménu terorismu. Postup práce se drží zadání a v následujících zmiňuje stručně historii terorismu, společně s jeho etapizací, která je převzata z publikace od Řeháka a Foltina.

Jejich etapizace je doplněna o návrh zakomponování nové etapy, která odráží aktuální bezpečnostní prostředí a vývoje terorismu.

Hlavním tématem jsou moderní formy terorismu – kybernetický terorismus a využívání bezpilotních letounů k útokům. Kybernetický terorismus je spojen s neustále se stupňujícími kybernetickými útoky. Tuto skutečnost potvrzuje ve své zprávě např. organizace Cifas a server infosecurity-magazine.com, které informují o tom, že ve Velké Británii bylo zaznamenáno za rok 2016 přes 325 tisíc podvodů, které byly spáchány prostřednictvím kybernetické sítě a byly cíleny na společnosti a veřejné instituce. Meziročně tak tento počet stoupl o čtyři procenta, což je znatelný nárůst. Ze všech zaznamenaných podvodů na území Velké Británie tvořily internetové podvody a útoky 60 procent, což jasně zvýrazňuje závažnost problému. Generální ředitel společnosti informoval o tom, že se v rámci jejich činnosti snaží počty kybernetických útoků snižovat, avšak útočníci mění své modus operandi a začínají více využívat kombinované útoky, kdy využívají telefonického spojení k získání osobních údajů, které dále využijí při svých útocích a podvodech v rámci kybernetické sítě. Z mnoha zdrojů lze tedy usuzovat stejný závěr – kybernetické útoky jsou vážným rizikem v současnosti a v budoucnosti budou zastávat roli stále větší. [59]V rámci zkoumání problému je potvrzován druhá hypotéza a to, že sofistikovanost prostředků k páchání teroristických činů.

Na téma kyberterorismu je v práci také uvedeno více definicí, jejich interpretace je v práci rozvinuta a jsou vysvětleny i související pojmy. V rámci diskuze je nutné zdůraznit skutečnost, že hranice mezi kybernetickým tenoristou a kybernetickým kriminálníkem, který jedná čistě za účelem zisku je často sporná či rozmazaná.

V další části práce jsou znázorněny prostředky kybernetického terorismu, metody útoků a propojení kybernetického prostorů a teroristických útoků. V rámci této podkapitoly je apelováno na nutnost adaptace bezpečnostního systému, neboť je potřeba, aby byli osoby odpovědné za kybernetickou bezpečnost vždy o krok napřed před útočníky, i když tomu v praxi často bývá naopak.

Kybernetické útoky mohou být vedeny na informační infrastrukturu z různých důvodů a na různé oblasti. Např. s cílem ochromení bezpečnostních složek či narušení dopravních kapacit. V následujícím obrázku budou zobrazeny různé typy útočníků a jejich motivace.

K narušení kybernetické bezpečnosti může dle Jirkovského (2007) dojít následujícími způsoby:

- Únikem informace**,** což je stav, kdy dojde k vyzrazení chráněné informace neautorizovanému subjektu.
- Narušením integrity, která představuje poškození, změnu, či vymazání dat.
- Potlačením služby - což znamená úmyslné bránění v přístupu k informacím, aplikacím, či systému. (Jde například o útoky typu DoS - Denial of Service resp. Jejich aktuální verze DDoS (Distributed Denial of Service - odmítnutí služby**)**, kdy dojde k zahlcení informačního kanálu nesmyslnými informacemi.
- Nelegitimním použití, což je užití informací neautorizovaným subjektem či neoprávněným způsobem (například dojde k napadení zpoplatněného systému a využívaní jeho služeb bez platby za služby) [70]

Následují bezpilotní letouny, které jsou rozebírány v teoretické části v další kapitole. Zde je také uvedena definice, typologie a využití dronů. Drony jsou stejně často probíraným a medializovaným fenoménem jako je kybernetický terorismus. Tisková mluvčí amerického Ministerstva vnitra uvedla ve svém prohlášení o bezpilotních letounech následující výrok: *„Zatímco mnohá setkání s drony nejsou nepříjemným zážitkem a mohou posloužit dobré věci, mnozí podceňují potenciální nebezpečí, které v sobě skrývají, a které by mohli nepřátelé využívat k jejich aktivitám.“* [54]

So Rastgaar, inženýr z Massachusettského technologického institutu (MIT) se o riziku využití bezpilotních letounů vyjadřuje následujícím způsobem: *„Když jsem při posledním projevu amerického prezidenta viděl všechny ty odstřelovače na střechách, říkal jsem si, jestli tak trochu nepodceňují rizika. S pistolí by proti němu dnes nikdo nešel. Ale s dronem?“* [53]

Autor práce s výše vyjádřenou obavou souhlasí a v práci za pomoci sesbíraných informací potvrzuje první hypotézu práce, která je podporována i dále v praktické části práce, kde jsou útoky bezpilotními letouny dále rozebírány a jsou vůči nim nastíněny možné prostředky obrany.

Bahenský se ve své diplomové práci, kterou zpracovával na téma využívání dronů vyjadřuje na téma rizik využívání dronů následovně: *„ Svět se v několika posledních letech hodně proměnil. Ve světě narůstá hrozba terorismu, zejména pak islámského. Pro teroristy znamená dron novou formu boje představující techniku, která je lehce k dostání. Například při nedávném incidentu v Paříži* [60], *kdy nad francouzskou metropolí létalo v noci pět dronů a policie nebyla schopna zjistit, kdo bezpilotní prostředky ovládal. Ve většině případů se zatím jedná především o zvědavost lidí nebo o provokace, kterých postupně přibývá. Tyto přelety ale vyvolávají obavy z*

možných teroristických útoků, kdy dron může zaútočit bombou nebo jedovatým plynem. Což představuje novou formu terorismu.“ [61]

Než budou v diskuzi zmíněné další závěry a poznatky z práce, je třeba zmínit i právní zakotvení práce v právních předpisech ČR i mezinárodních dokumentech. V práci jsou zmíněny vybrané právní předpisy a dokumenty a je stručně za pomocí tabulek vysvětlen jejich obsah. Zkoumání právních dokumentů se soustředilo na oblast terorismu, kybernetického terorismu a kybernetické bezpečnosti a v neposlední řadě na problematiku právní úpravy užívání bezpilotních letounů. Vznikl tak ucelený přehled právních pramenů týkající se zkoumané problematiky.

V úvodní části praktické části jsou vyobrazeny grafy, které znázorňují vývoj teroristických aktivit v západní Evropě. Jsou zde zobrazeny počty obětí a podíl islamistických teroristů na páchaných útocích.

Následuje praktická část, která je věnována kybernetickým útokům. V první části jsou zmíněny týmy a sdružení odborníků, které mají pomáhat k eliminaci a ke zmírňování následků kybernetických útoků. V grafickém znázornění je ilustrován nárůst kybernetických útoků na území USA z důvodu ilustrování globálnosti problému a skutečnosti, že vyspělé země jsou tímto fenoménem nejvíce ohroženy.

Další část slouží k dalšímu potvrzování druhé hypotézy, neboť jsou v ní uvedena další grafická vyobrazení, kde je zřejmý nárůst využívání bezpilotních letounů k vojenským zásahům. Úměrně roste i počet využívání dronů protistranou. Další graf zobrazuje predikci nárůstu využívání dronů, čímž jsou dále potvrzovány hypotézy.

V rámci případových studií jsou v práci zmíněny jedny z nejvýznamnějších kybernetických útoků, jejich viníci a následky. Studie jsou stručné a mají identickou strukturu složenou vždy z popisu útoku, použitých prostředků, důsledků útoků a na závěr označují viníka či útočníka.

V další kapitole práce jsou uvedeny doporučení pro zvýšení kybernetické bezpečnosti ve zkoumaných společnostech. V rámci zkoumáni jsou identifikovány problémy ve zkoumaných společnostech, mezi které patří:

- Nedokonale nastavená uživatelská práva (chyba lidského faktoru)
- Málo rozvinutá komunikace mezi zaměstnanci a IT oddělením
- Kvalitní antivirové řešení a monitoring konečných stanic
- Kontrola externích firem, které spolupracují se společností
- Správné nastavení zpětné vazby (feedback)
- Ochrana serverů a citlivých míst
- Zapojení se do projektů ke zvýšení kybernetické bezpečnosti
- Ochrana hardwaru a softwaru společnosti před vestavěnými prostředky k útoku

U každého identifikovaného problému je navrhnuto opatření ke zvýšení bezpečnosti. Dokument Národní strategie kybernetické bezpečnosti České republiky na období let 2015 až 2020 zobrazuje mnohé výše uvedené problémy a řešení ve svých výzvách a cílech. Často je zde nutné pouze substituovat stát za společnost a cíle jsou v určitých ohledech velmi podobné.

Jedná se například o body vizí a cílů:

- Nedostatečná důvěra veřejnosti ve stát - souvisí se správným nastavením zpětné vazby (feedback)

- Možnosti zneužití zadních vrátek hardware pro exfiltraci informací - souvisí s ochranou hardwaru a softwaru společnosti před vestavěnými prostředky k útoku
- Nedostatečné zabezpečení malých a středních podniků - souvisí s kvalitním antivirovým řešením a monitoringem konečných stanic
- Botnety a DDoS/DoS útoky - souvisí s ochranou serverů a citlivých míst
- Nedostatek odborníků na kybernetickou bezpečnost a nutnost revize stávajících studijních programů ve školství - souvisí se zapojení se do projektů ke zvýšení kybernetické bezpečnosti[26]

Poslední rozsáhlejší kapitola se zabývá ochranou objektů před bezpilotními letouny. Nejdříve je popsán současný stav, který není zobrazen jako zcela ideální. V úvodu je taky zmíněn fakt, že účinné technologie na ochranu před útoky bezpilotními letouny jsou stále ve vývoji. V následující části je definován záměr společnosti neideální situaci změnit.

V podkapitole je zdůrazněno rozdílné řešení ochrany civilních a vojenských objektů, s tím, že tato část práce se bude soustředit na ochranu civilních objektů. Nicméně jsou v této části popsány vojenské řešení ochrany objektů za pomocí raketových systémů a jsou uvedeny příklady, jak a kdy byly tyto systémy využity. Je zde taky zmíněn faktor odůvodněného použití raketové ochrany. Ochrana raketovým systémem je jako řešení zavrženo zaprvé z výše uvedeného důvodu – zkoumaný objekt je civilního a nikoliv vojenského charakteru. Zadruhé je zde vyzdvihnuta značná ekonomická náročnost, která by pro zkoumanou společnost nebyla efektivní cestou.

Dále je popsáno aktuálně připravované řešení, které bude v blízké době uvedeno do provozu. Jedná se o systém ARDRONIS od společnosti R&S. Jsou

zde uvedeny výhody systému i jeho nevýhody. V tabulce v této části jsou zobrazeny formy řešení. Je identifikován způsob aktuálního řešení a řešení budoucího. V současné době se tedy navrhuje využívání řešení R&S ADRONIS-D Direction, které disponuje možnosti identifikace a zaměření bezpilotních letounů. Později bude proveden upgrade na systém R&S ADRONIS-P Protection, který navíc má možnost provádění protiopatření. V další tabulce je znázorněna plánovaná dostupnost konečného řešení.

V další podkapitole jsou navržena alternativní a souběžná opatření objektu před bezpilotními letouny. První alternativou je platforma SKYWALL 100, která představuje ruční mobilní řešení pro palbu sítí k eliminaci bezpilotních letounů. U každého navrhovaného řešení jsou uvedeny jejich výhody a nevýhody. U první alternativy jsou klady adaptability řešení, ekonomičnost, přesnost a nevýhodou je nutnost přiblížit se k cíli na poměrně krátkou vzdálenost a nemožnost využití proti všem typům dronů, avšak tuto nevýhodu mají společné takřka všechny řešení.

Následující řešení je představeno jako metoda boje „ohněm proti ohni“ a využívá postavení jednoho bezpilotního letounu vůči druhému. Je zde zdůrazněná podmínka, aby obranný dron byl vždy vyspělejší než protějšek, který podniká útok. Je zde uveden dron typu Falcon, který je k tomuto řešení sestaven, avšak v rámci komerční sféry lze nalézt i další řešení. U zmíněného řešení je podotknuto, že není v podmínkách zkoumané společnosti zcela vhodné, kvůli jeho možnostem zneužití. Současně je však zmíněn způsob, jak tuto nevýhodu eliminovat. I když se nezachová původní funkce.

Dalším zmíněným řešením je GPS restrikce letounů takovým způsobem, aby se do určitých míst, jako jsou mezinárodní letiště (zkoumaný objekt) a vojenské základy, nemohli v rámci továrního nastavení dostat. Je také uvedena

skutečnost, že tato ochrana nemusí být zcela účinná, ale dokáže eliminovat velkou část nehod.

Autor vyjadřuje své sympatie vůči řešení ochrany objektu za pomoci přirozených predátorů vzdušného prostoru a to jsou dravci. Zkoumaný objekt dravci disponuje a pouhým vycvičením od specializované firmy by mohl poměrně jednoduše tuto ochranu získat a rozvíjet. Společnost, která výcvik nabízí, poskytuje i zaškolení personálu, který na práci s dravci není vyškolen a dokonce i prodej vycvičeného dravce / dravců.

V rámci diskuze je nutné zmínit fakt, že toto řešení je oblíbené u mnoha policejních a vojenských hodnostářů. Vrchní komisař londýnské metropolitní policie Bernard Hogan-Howe o pořízení letky dravců uvažuje a o využití dravců prohlásil, že: *„Je to ideální low-tech řešení na hi-tech problém.“* [53]

K tomuto řešení je připojeno další, které navrhuje využití a vycvičení specializované jednotky, které působí v rámci zkoumané společnosti na sestřelování bezpilotních letounů, neboť disponuje dlouhými zbraněmi, které jsou uzpůsobené ke střelbě na pohybující se cíl.

Posledním navrhovaným řešením je alternativa k řešení od společnosti R&S ARDRONIS. Obdobné řešení nabízí například společnost Blighter, který svůj systém nazývá AUDS (Anti-UAV Defence System) a opravdu funguje na podobné bázi jako řešení výše uvedené, avšak je na rozdíl od řešení R&S v některých variantách mobilní. Avšak výhoda mobility je na druhou stranu zastíněna cenou řešení, která je neúměrně vyšší. Upřednostnění řešení od společnosti Blighter nepřispívá ani skutečnost, že instalace jiných systémů od jmenované společnosti se v prostředí zkoumané společnosti netěší nejlepším recenzím a ohlasům.

7 ZÁVĚR

Cílem práce bylo zmapovat bezpečnostní prostředí a jeho připravenost na teroristické útoky. Využitím většího počtu metod byl vypracován ucelený přehled právních předpisů s jejich charakteristikou. V průběhu práce byly ověřovány stanovené hypotézy, které byly postupným zkoumáním potvrzovány. Jako hlavní přednost a přínos práce lze identifikovat praktickou část práce, kde jsou přehledně uvedené u tématu kybernetického terorismu uvedeny nejvýznamnější útoky, které byly dosud provedeny, je u nich uvedena jejich charakteristika, původce a reakce na tyto útoky, které vedly k zdokonalení systému ochrany před takovými útoky. Dále byli ve zkoumaných společnostech identifikovány problémy, ke kterým bylo taktéž navrhnuto řešení. Tyto řešení se v určité formě shoduj s koncepčními dokumenty pro zvýšení kybernetické bezpečnosti v rámci ČR, jak je uvedeno v diskuzi.

Dalším tématem uvedeným v praktické části jsou bezpilotní letouny, u nich je stejně jako u kyberterorismu definován právní rámec, uvedena typologie a pomocí grafického vyobrazení znázorněna stoupající tendence jejich využívání. Důležitou součástí této části jsou návrhy řešení pro zvýšení bezpečnosti zkoumaného objektu proti útokům bezpilotních letounů. Zde byly navrženy různé způsoby řešení a posouzeny jejich výhody a nevýhody. V průběhu praktické části byly zkoumáním potvrzovány stanovené hypotézy.

Autor by si na závěr práce dovolil zmínit paradox, který ovlivňuje bezpečnostní oblast. Každý odborník hlásá, že prevence je nejlepší způsob řešení problémů, avšak v bezpečnostní oblasti se často jedná, až po útoku, který ohrozí či poničí chráněné zájmy. Omluva bývá totiž často levnější, než funkční řešení. Autor nabádá ke změně tohoto přístupu.

8 SEZNAM POUŽITÝCH ZKRATEK

MVČR	Ministerstvo vnitra České republiky
FBI	Americký Federální úřad pro vyšetřování (Federal Bureau of Investigation)
CIA	Ústřední zpravodajská služba USA (Central Intelligence Agency)
VPN	Virtuální privátní síť (Virtual Private Network)
TOR	The Onion Router
IS	Islámský stát
MO	Modus operandi
BIS	Bezpečnostní informační služba
CSIRT	Tým pro reakce na bezpečnostní incidenty (Computer Security Incident Response Team)
CERT	Tým pro reakci na kybernetické nouzové situace (Computer Emergency Response Team)
GovCERT	vládní Computer Emergency Response Team
ICAO	Mezinárodní organizace pro civilní letectví (International Civil Aviation Organization)
EASA	Evropská agentura pro bezpečnost letectví (European Aviation Safety Agency)
FAA	Federální letecká správa (Federal Aviation Administration)
ISP	Poskytovatel internetového připojení
MitM	Útok s prostředníkem (Man in the middle)

MIT	Massachusettský technologický institut (Massachusetts Institute of Technology)
BOL	Biologická ochrana letiště
UAC	Řízení uživatelských účtů (User Account Control)

9 SEZNAM POUŽITÉ LITERATURY

[1] Definice pojmu terorismus. Http://www.mvcr.cz [online]. 2009 [cit. 2017-05-06]. Dostupné z: http://www.mvcr.cz/clanek/definice-pojmu-terorismus.aspx

[2] Terorismus. Http://www.mvcr.cz [online]. 2017 [cit. 2017-05-06]. Dostupné z: http://www.mvcr.cz/cthh/clanek/terorismus-web-uvod-terorismus.aspx

[3] Trestně-právní úprava terorismu. Http://www.mvcr.cz [online]. 2010 [cit. 2017-05-08]. Dostupné z: http://www.mvcr.cz/clanek/trestne-pravni-uprava-terorismu.aspx

[4] Zákon č. 40/2009 Sb.: Zákon trestní zákoník. Https://www.zakonyprolidi.cz [online]. 2009 [cit. 2017-05-07]. Dostupné z: https://www.zakonyprolidi.cz/cs/2009-40

[5] BRZYBOHATÝ, Marian. Současné vývojové trendy terorismu a vybrané pedagogické problémy výcviku speciálních jednotek. Vyd. 1. Praha: Policejní akademie České republiky, 2001, 8 s. ISBN 80-725-1073-8.

[6] Historický vývoj terorismu. Http://www.obranaastrategie.cz [online]. 2017 [cit. 2017-05-10]. Dostupné z: http://www.obranaastrategie.cz/cs/archiv/rocnik-2006/1-2006/historicky-vyvoj-terorismu.html#.WRK6I2nyjcs

[7] ŠEDIVÝ, J. Nové paradigma terorismu. Mezinárodní politika. Praha, 2003, roč. 4, č. 1, ISSN 0543-7962.

[8] ŘEHÁK, David, Pavel FOLTIN a Richard STOJAR. Vybrané aspekty soudobého terorismu. Praha: Ministerstvo obrany České republiky - Agentura vojenských informací a služeb, 2008. ISBN 978-80-7278-443-1.

[9] Kyberneticky terorismus, kyberterorismus. Http://www.mvcr.cz/ [online]. 2010 [cit. 2017-02-17]. Dostupné z: http://www.mvcr.cz/clanek/kyberneticky-terorismus-kyberterorismus.aspx

[10] JOHNATAN, Matusitz. Cyberterrorism. American Foreign Policy Interests. 2005, (2), s. 137

[11] DENNING, D. E. [cit. 2017-05-07]. Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy, [online]. Dostupné z: http://www.nautilus.org/infopolicy/workshop/papers/denning.html

[12] Zákon o kybernetické bezpečnosti. Www.kybernetickyzakon.cz [online]. 2015 [cit. 2017-05-13]. Dostupné z: http://www.kybernetickyzakon.cz/

[13] Prováděcí právní předpisy k zákonu č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). Národní bezpečnostní úřad [online]. 2014 [cit. 2016-03-12]. Dostupné z: http://www.nbu.cz/cs/pravni-predpisy/provadeci-pravni-predpisy/provadeci-pravni-predpisy-k-zakonu-c-1812014-sb-o-kyberneticke-bezpecnosti-a-o-zmene-souvisejicich-zakonu/

[14] Zákon 365/2000 Sb. O informačních systémech veřejné správy. Http://www.pristupnost.cz/ [online]. 2000 [cit. 2016-03-06]. Dostupné z: http://www.pristupnost.cz/pristupnost-webu-statni-spravy/zakon-365-2000-sb-o-informacnich-systemech-verejne-spravy/

[15] Zpráva TE-SAT 2016. Http://www.mvcr.cz [online]. 2016 [cit. 2017-05-08]. Dostupné z: http://www.mvcr.cz/cthh/clanek/terorismus-web-dokumenty-dokumenty.aspx

[16] Unmanned Aircraft Systems (UAS). Http://www.icao.int [online]. 2011 [cit. 2017-05-09]. Dostupné z: http://www.icao.int/Meetings/UAS/Documents/Circular%20328_en.pdf

[17] Unmanned aerial vehicle. Http://www.thefreedictionary.com [online]. 2005 [cit. 2017-05-12]. Dostupné z: http://www.thefreedictionary.com/Unmanned+Aerial+Vehicle

[18] Strategie České republiky pro boj proti terorismu od r. 2013. Www.mvcr.cz [online]. 2016 [cit. 2017-05-14]. Dostupné z: http://www.mvcr.cz/clanek/dokumenty-454055.aspx

[19] USNESENÍ VLÁDY ČESKÉ REPUBLIKY ze dne: 13. září 2006 č. 1060. Https://albatros.vlada.cz [online]. 2006 [cit. 2017-05-14]. Dostupné z: https://albatros.vlada.cz/usneseni/usneseni_webtest.nsf/9d960a7bf947adf0c1256c8a00755e91/d93d0ff32f9846dac12571e8004b2b82?OpenDocument

[20] Zákon č. 153/1994 Sb. Zákon o zpravodajských službách České republiky. Https://www.zakonyprolidi.cz [online]. 1994 [cit. 2017-05-14]. Dostupné z: https://www.zakonyprolidi.cz/cs/1994-153

[21] Boj EU proti terorismu. Http://www.consilium.europa.eu [online]. 2016 [cit. 2017-05-14]. Dostupné z: http://www.consilium.europa.eu/cs/policies/fight-against-terrorism/

[22] EU TERRORISM SITUATION & TREND REPORT (TE-SAT). Www.europol.europa.eu [online]. 2016 [cit. 2017-05-14]. Dostupné z: https://www.europol.europa.eu/activities-services/main-reports/eu-terrorism-situation-and-trend-report

[23] Zákon č. 365/2000 Sb. Zákon o informačních systémech veřejné správy a o změně některých dalších zákonů. Https://www.govcert.cz [online]. 2000 [cit. 2017-05-15]. Dostupné z: https://www.zakonyprolidi.cz/cs/2000-365

[24] Zákon č. 127/2005 Sb. Zákon o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích). Www.zakonyprolidi.cz [online]. 2005 [cit. 2017-05-15]. Dostupné z: https://www.zakonyprolidi.cz/cs/2005-127

[25] VYHLÁŠKA O KYBERNETICKÉ BEZPEČNOSTI. Https://www.govcert.cz [online]. [cit. 2017-05-15]. Dostupné z: https://www.govcert.cz/cs/faq/vyhlaska-o-kyberneticke-bezpecnosti/

[26] STRATEGIE / AKČNÍ PLÁN. Https://www.govcert.cz [online]. 2015 [cit. 2017-05-15]. Dostupné z: https://www.govcert.cz/cs/informacni-servis/strategie-akcni-plan/

[27] NATO má první manuál na vedení kybernetické války. Mediální proroci [online]. 2015, 2015 [cit. 2015-11-19]. Dostupné z: http://medialniproroci.blogspot.cz/2013/04/nato-ma-prvni-manual-na-vedeni.html

[28] Tallinn Manual. Cooperative Cyber Defence Centre of Excellence [online]. 2015 [cit. 2016-03-01]. Dostupné z: https://ccdcoe.org/research.html

[29] National Cyber Security Strategy 2016 to 2021. Www.gov.uk [online]. 2016 [cit. 2017-05-15]. Dostupné z: https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021

[30] Zákon č. 49/1997 Sb. Zákon o civilním letectví a o změně a doplnění zákona č. 455/1991 Sb., o živnostenském podnikání (živnostenský zákon), ve znění pozdějších předpisů. Https://www.zakonyprolidi.cz [online]. 1997 [cit. 2017-05-15]. Dostupné z: https://www.zakonyprolidi.cz/cs/1997-49

[31] PŘEDPIS L 2 - DOPLNĚK X – BEZPILOTNÍ SYSTÉMY. Lis.rlp.cz [online]. 2014 [cit. 2017-05-15]. Dostupné z: http://lis.rlp.cz/predpisy/predpisy/dokumenty/L/L-2/data/effective/doplX.pdf

[32] Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů. Https://www.zakonyprolidi.cz [online]. 2000 [cit. 2017-05-15]. Dostupné z: https://www.zakonyprolidi.cz/cs/2000-101

[33] STANOVISKO č. 1/2013 Úřadu pro ochranu osobních údajů. Https://www.uoou.cz [online]. 2013 [cit. 2017-05-15]. Dostupné z: https://www.uoou.cz/files/stanovisko_2013_1.pdf

[34] Dokument D 122. Http://www.aaao.cz [online]. 2014 [cit. 2017-05-15]. Dostupné z: http://www.aaao.cz/upload/root/aktuality/eu/2014/dokument_d_122_legislativa_drony.pdf

[35] Nařízení Evropského parlamentu a Rady (ES) č. 785/2004 ze dne 21. dubna 2004 o požadavcích na pojištění u leteckých dopravců a provozovatelů letadel. Http://eur-lex.europa.eu [online]. 2004 [cit. 2017-05-

15]. Dostupné z: http://eurlex.europa.eu/legal content/CS/TXT/?uri=CELEX%3A32004R0785

[36] Drony, bezpečnostní hrozba? Https://www.securityguide.cz [online]. 2016 [cit. 2017-05-14]. Dostupné z: https://www.securityguide.cz/drony-bezpecnostni-hrozba/

[37] Literární rešerše. Http://www3.econ.muni.cz [online]. 2017 [cit. 2017-05-10]. Dostupné z: http://www3.econ.muni.cz/~99246/zav-prace/lit-review.xhtml

[38] Metodika závěrečné práce. Lorenc. [online]. [cit. 2017-04-30]. Dostupné z: http://lorenc.info/zaverecne-prace/metodika.htm

[39] Statistika: Počty obětí teroristických útoků v západní Evropě v letech 1970-2015. Http://eurodenik.cz [online]. 2016 [cit. 2017-05-15]. Dostupné z: http://eurodenik.cz/zpravy/statistika-pocty-obeti-teroristickych-utoku-v-zapadni-evrope-v-letech-19702015

[40] CO JE NCKB. Národní centrum kybernetické bezpečnosti [online]. 2011 [cit. 2017-05-16]. Dostupné z: http://www.govcert.cz/

[41] Csirt.cz. CSIRT.CZ [online]. 2017 [cit. 2017-05-16]. Dostupné z: https://csirt.cz/

[42] CERT/CSIRT týmy a jejich role. Https://www.root.cz [online]. 2013 [cit. 2017-05-16]. Dostupné z: https://www.root.cz/clanky/cert-csirt-tymy-a-jejich-role/

[43] Význam ransomware. Www.vyznam-slova.com [online]. 2016 [cit. 2017-05-16]. Dostupné z: http://www.vyznam-slova.com/ransomware

[44] Cyber security infographic. Http://www.nato.int [online]. 2013 [cit. 2017-05-16]. Dostupné z: http://www.nato.int/docu/review/2013/cyber/Cyber-Security-in-Focus/EN/index.htm

[45] Britain's Drone Secrets. Http://www.globalresearch.ca [online]. 2013 [cit. 2017-05-16]. Dostupné z: http://www.globalresearch.ca/britains-drone-secrets/5325997

[46] DRONE TECHNOLOGY FROM HUMAN SECURITY PERSPECTIVE. Http://www.cbap.cz [online]. 2017 [cit. 2017-05-16]. Dostupné z: http://www.cbap.cz/archiv/3477

[47] Department of Transportation Report Estimates 250,000 Drones in US Airspace by 2035. Leaksource.wordpress.com [online]. 2013 [cit. 2017-05-16]. Dostupné z: https://leaksource.wordpress.com/2013/11/24/department-of-transportation-report-estimates-250000-drones-in-us-airspace-by-2035/

[48] The world's 10 most dangerous cyberwarfare attacks. Techworld.com [online]. 2016 [cit. 2017-03-06]. Dostupné z: http://www.techworld.com/security/worlds-10-most-dangerous-cyberwarfare-attacks-3601660/

[49] WHAT IS A ZERO-DAY EXPLOIT. Www.fireeye.com [online]. 2016 [cit. 2017-03-07]. Dostupné z: https://www.fireeye.com/current-threats/what-is-a-zero-day-exploit.html

[50] Protiletadlový systém Pečora–2M sestřelil v Sýrii špičkový americký dron MQ-1 Predator. Http://www.eurasia24.cz [online]. 2017 [cit. 2017-05-17]. Dostupné z: http://www.eurasia24.cz/vojenstvi/item/2413-protiletadlovy-system-pecora-2m-sestrelil-v-syrii-spickovy-americky-dron-mq-1-predator

[51] Spojenci USA zničili 200 dolárového drona raketou za 3 milióny. Https://androidportal.zoznam.sk [online]. 2017 [cit. 2017-05-17]. Dostupné z: https://androidportal.zoznam.sk/2017/03/spojenci-usa-znicili-200-dolaroveho-drona-raketou-3-miliony/

[52] ARDRONIS Automatic Radio-controlled Drone Identification Solution. Www.rohde-schwarz.com [online]. 2017 [cit. 2017-05-16]. Dostupné z: https://www.rohde-schwarz.com/us/products/monitoring-and-network-testing/ardronis/pg_overview_230808.html

[53] Dravci, rušičky, sítě: jak sundat nebezpečný dron z oblohy. Xman.idnes.cz [online]. 2016 [cit. 2017-05-17]. Dostupné z: https://xman.idnes.cz/jak-sestrelit-dron-terorismus-dz2-/xman-styl.aspx?c=A160317_150941_xman-styl_fro

[54] SkyWall CAPTURE DRONES - PROTECT ASSETS. SkyWall100 MAN PORTABLE DRONE DEFENCE [online]. 2017 [cit. 2017-05-17]. Dostupné z: https://openworksengineering.com/skywall

[55] Michigan Tech: To Catch a Drone, Send a Drone. Http://dronelife.com [online]. 2016 [cit. 2017-05-17]. Dostupné z: http://dronelife.com/2016/01/22/michigan-tech-to-catch-a-drone-send-a-drone/

[56] FAA's new drone program goes above and beyond the line of sight. Http://newatlas.com [online]. 2016 [cit. 2017-05-17]. Dostupné z: http://newatlas.com/faa-pathfinder-program-drone/37396/#gallery

[57] AUDS Anti-UAV Defence System. Http://www.blighter.com [online]. 2016 [cit. 2017-05-17]. Dostupné z: http://www.blighter.com/products/auds-anti-uav-defence-system.html

[58] MOGHADDAM F.: The Staircase to Terrorism: A Psychological Exploration. American Psychologist, February-March, Georgetown 2005, s. 161 – 169, [online]. 2005 [cit. 2017-12-05]. Dostupný z WWW:< http://www.sonoma.edu/users/s/smithh/psy326/moghaddam.pdf

[59] DVĚ TŘETINY PODVODŮ V BRITÁNII LONI PROBĚHLY ONLINE. Http://www.dvojklik.cz [online]. 2017 [cit. 2017-05-17]. Dostupné z: http://www.dvojklik.cz/dve-tretiny-podvodu-v-britanii-loni-probehly-online?utm_source=fb&utm_medium=post&utm_content=dvojklik&utm_campaign=sa10

[60] ŠERÝ, Miloslav. Regionální geografie Afriky. Olomouc: Univerzita Palackého, Přírodovědecká fakulta, katedra geografie. Dostupné také z: http://distgeo.upol.cz/uploads/vyuka/skripta-sery.pdf

[61] BAHENSKÝ, Pavel. The Use of Drones in Air Cargo Transportation. Prague, 2015. Diploma thesis. CTU, Faculty of Transportation Sciences. Supervisor Ing. Viktor Sýkora, Ph.D.

[62] START_GlobalTerrorismDatabase. Www.start.umd.edu [online]. 2015 [cit. 2017-05-17]. Dostupné z: http://www.start.umd.edu/gtd/images/START_GlobalTerrorismDatabase_2015TerroristAttacksConcentrationIntensityMap.jpg

[63] Předpisy pro létání s drony v ČŘ. Http://www.droneweb.cz [online]. 2016 [cit. 2017-05-15]. Dostupné z: http://www.droneweb.cz/legislativa-provozu-dronu/item/37-predpisy-pro-letani-s-drony-v-cr

[64] Vojenské využití Dronu DJI MAVIC (ISIS a využití civilních dronů k vojenským účelům. Http://www.droneweb.cz [online]. 2017 [cit. 2017-05-

15]. Dostupné z: http://www.droneweb.cz/vojenske-drony/item/135-isis-a-vyuziti-civilnich-dronu-k-vojenskym-ucelum)

[65] This drone catches other drones by shooting nets at them. Www.rt.com [online]. 2016 [cit. 2017-05-17]. Dostupné z: https://www.rt.com/usa/328577-drone-catcher-net-interceptor/

[66] Drone-hunting eagles can snatch devices out of the sky. /www.cbsnews.com [online]. 2016 [cit. 2017-05-17]. Dostupné z: http://www.cbsnews.com/news/drone-hunting-eagles-can-snatch-the-devices-out-of-the-sky/

[67] Justice is Served: Idiot Fined $850 For Shooting Down Drone. Dronelife.com [online]. 2016 [cit. 2017-05-17]. Dostupné z: http://dronelife.com/2015/07/03/justice-is-served-idiot-fined-850-for-shooting-down-drone/

[68] Small drone 'shot with Patriot missile. Www.bbc.com [online]. 2016 [cit. 2017-05-17]. Dostupné z: http://www.bbc.com/news/technology-39277940

[69] Naval Open Source INTelligence. *Nosint.blogspot.cz/* [online]. 2016 [cit. 2017-05-17]. Dostupné z: http://nosint.blogspot.cz/

[70] JIROVSKY, V. Kybernetická kriminalita nejen o hackingu, crackingu, virech a trojských koních bez tajemství. Praha: Grada Publishing, a. s., 2007. s. 21 a nasl.

[71] *The DROWN Attack* [online]. 2016 [cit. 2017-05-06]. Dostupné z: https://drownattack.com/

[72] How To Test SSLv2 DROWN Attack Vulnerability Using Python Script (And Solution to Fix the DROWN Attack on Apache and NginX). *Thegeekstuff.com* [online]. 2016 [cit. 2016-03-06]. Dostupné z: https://thegeekstuff.com

10 SEZNAM POUŽITÝCH TABULEK

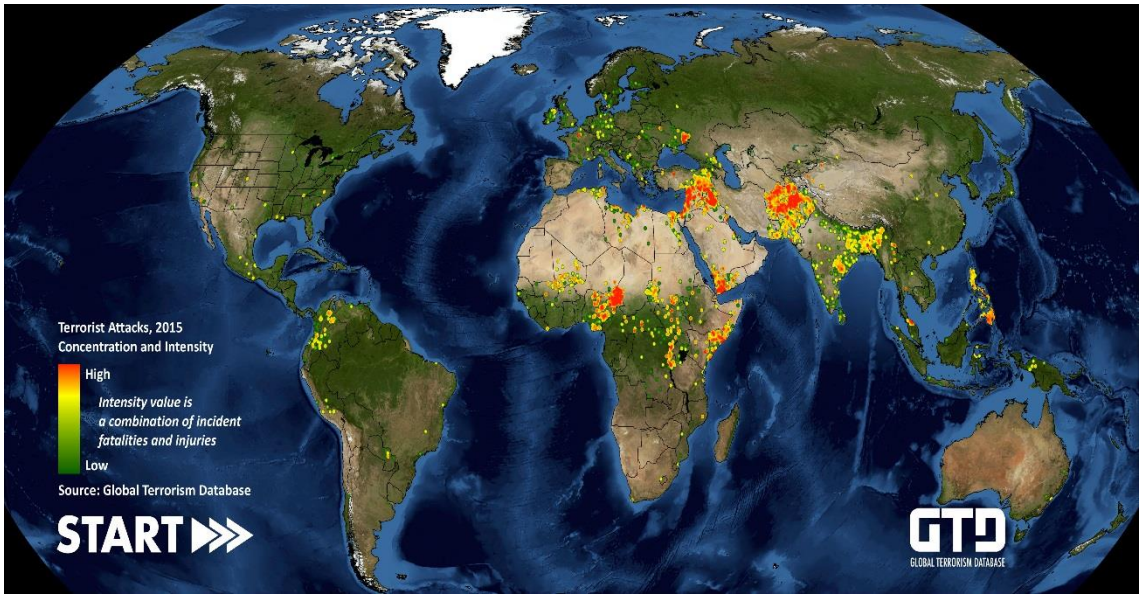
11 SEZNAM POUŽITÝCH GRAFŮ

12 SEZNAM PŘÍLOH

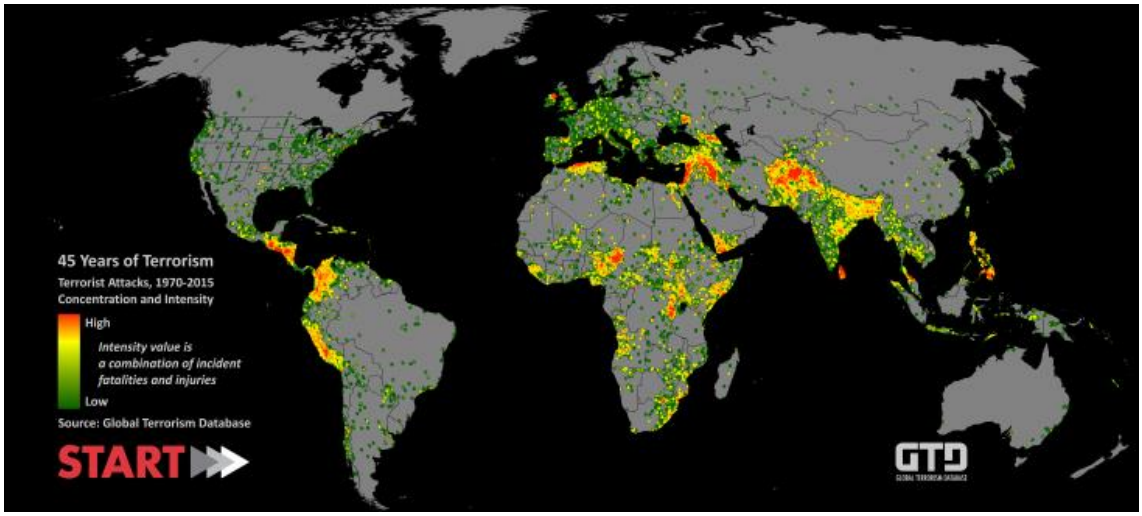
PŘÍLOHY

Příloha 1

Mapy teroristických aktivit



Obrázek 1 Mapa teroristických činů v globálním měřítku za rok 2015 [62]



Obrázek 2 Mapa teroristických činů v globálním měřítku za období 1970-2015 (45 let) [62]

Příloha 2

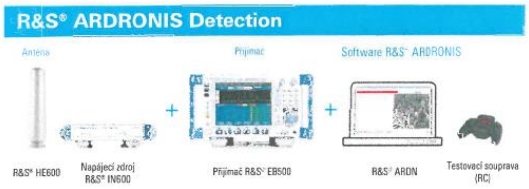
Specifikace jednotlivých systémů ADRONIS

Pasivní přístup

R&S® ARDRONIS-I

Rychlá, spolehlivá **identifikace** rádiového vysílání ovládacích povelů mikrodronů:

- Robustní detekce a identifikace signálu
- Rychlá odezva a včasné varování
- Automatické spouštění alarmu
- Přehled o celém kmitočtovém spektru
- Snadno použitelné a plně automatizované, integrované workflow
- Rozšiřovatelná databáze profilů
- Výkonný, kompaktní systém
- Snadný transport



Aktivní přístup

R&S® ARDRONIS-R

Identifikace a **protiopatření**. Okamžité působení proti hrozbám pocházejícím z detekovaných rádiem ovládaných mikrodronů:

- Zahrnuje všechny funkce identifikace mikrodronů (R&S® ARDRONIS-I)
- Přeruší spojení mezi dálkovým ovladačem a dronem
- Reakční a selektivní rušení každé jednotlivé linky dálkového ovládání (RC)
- Přesná protiopatření s minimálním výstupním výkonem
- Ostatní signály v kmitočtovém pásmu nejsou ovlivněny
- Automatické rušení na základě profilů detekce
- Brání dronům proniknout do chráněné oblasti

Obrázek 3 Specifikace jednotlivých systémů ADRONIS-I a ADRONIS R [52]

R&S® ARDRONIS-D

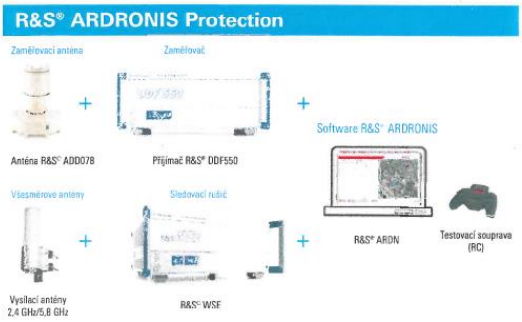
Souběžná pokročilá **identifikace** a **zaměřování** rádiových linek dálkového ovládání (RC):

- Zahrnuje všechny funkce identifikace mikrodronů (R&S® ARDRONIS-I)
- Přesné zaměřování aktivních dálkových ovladačů a mikrodronů
- Zaměřování s vysokou citlivostí
- Vynikající přesnost zaměřování a odolnost proti odrazům
- Rychlé zaměření dronů FHSS/DSSS s vysokou pravděpodobností zachycení
- Integrovaná elektronická mapa
- Zobrazení videostreamu
- Otevřené rozhraní, interoperabilní a upravitelné

R&S® ARDRONIS-P

Rozsáhlé řešení typu „vše v jednom" ochrany před hrozbami pocházejícími z rádiem ovládaných mikrodronů:

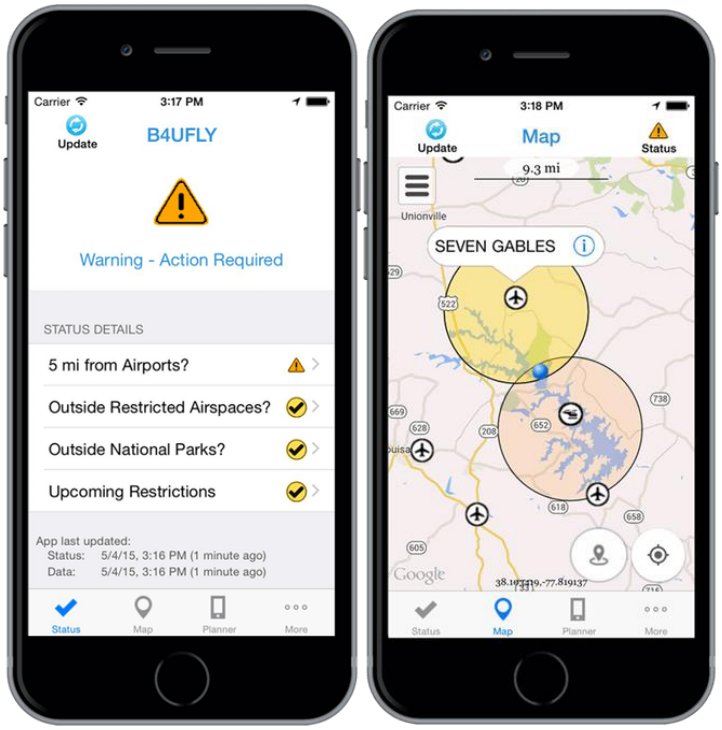
- Zahrnuje všechny funkce identifikace mikrodronů, jejich zaměřování a protiopatření vůči nim (R&S® ARDRONIS-I/-D/-R)



Obrázek 4 Specifikace jednotlivých systémů ADRONIS-D a ADRONIS P [52]

Příloha 3

Názorná ukázka prostředí ovládání na základě restrikce za pomoci GPS



Obrázek 5 Ukázka prostředí ovládání na základě restrikce (GPS) – checklist a mapa [56]

Obrázek 6 Ukázka prostředí ovládání na základě restrikce (GPS) – plánovač a mapa [56]

Příloha 4

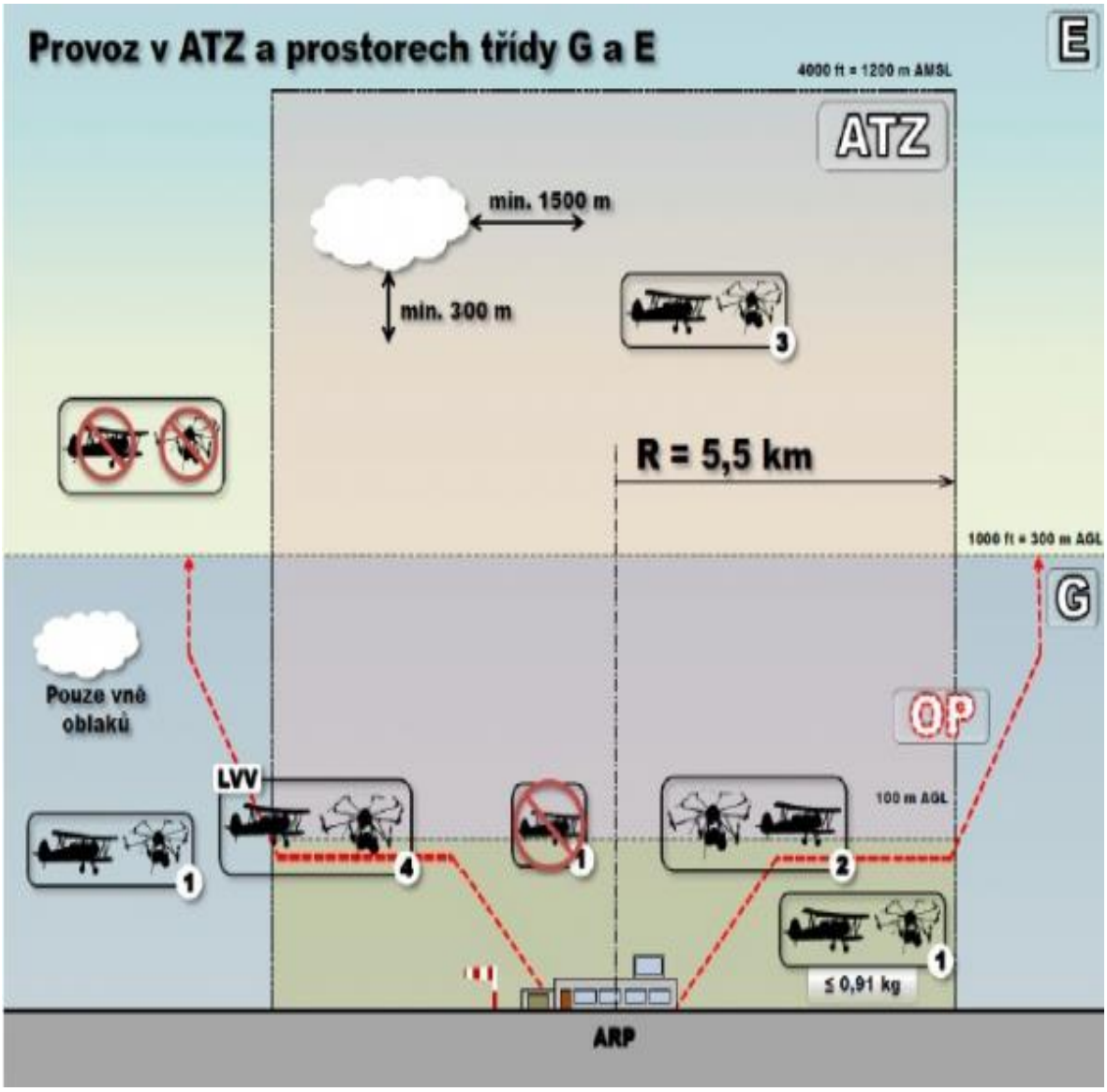
Tabulka povinnosti při provozování bezpilotního letounu

Tabulka 1 (viz ust. 16)										
ř.	maximální vzletová hmotnost	≤ 0,91 kg		> 0,91 kg a < 7 kg		7 – 20 kg		> 20 kg		bezpilotní letadlo provozované mimo dohled pilota
-	účel použití / požadavek	rekreačně sportovní	výdělečné, experimentální, výzkumné	rekreačně sportovní	výdělečné, experimentální, výzkumné	rekreačně sportovní	výdělečné, experimentální, výzkumné	rekreačně sportovní	výdělečné, experimentální, výzkumné	
1	evidence letadla	ne	ano	ne	ano	ne	ano	ano	ano	ano
2	evidence pilota	ne	ano	ne	ano	ne	ano	ano	ano	ano
3	praktický a teoretický test pilota	ne	ano	ne	ano	ne	ano	ano	ano	ano
4	povolení k létání	ne	ano	ne	ano	ne	ano	ano	ano	ano
5	povolení k provádění LP a LČPVP	nelze	ano	nelze	ano	nelze	ano	nelze	ano	nelze
6	označení UA: ID štítek / ID štítek + pozn. značka	ne / ne	ano / ano	ano / ne	ano / ano	ano / ne	ano / ano	ano / ne	ano / ano	ano / ano
7	min. ve vzdálenosti (m): vzlet, přistání / osoby, stavby / osídlený prostor	bezpečná	bezpečná	bezpečná	bezpečná	bezpečná, ale minimálně 50/100/150	bezpečná, ale minimálně 50/100/150	bezpečná, ale minimálně 50/100/150	bezpečná, ale minimálně 50/100/150	bezpečná, ale minimálně 50/100/150
8	pojištění: běžný provoz / LVV (mil. Kč)	ne / 0,25	dle nař. č. 785/2004[1]	ne / 1	dle nař. č. 785/2004[1]	ne / 3	dle nař. č. 785/2004[1]	dle nař. č. 785/2004[1]	dle nař. č. 785/2004[1]	dle nař. č. 785/2004[1]
9	dozor	ne	ne	ne	ne	ne	ne	ano	ano	ne
10	„failsafe" systém	ne	ano	ano	ano	ano	ano	ano	ano	ano
11	provozní příručka UAS	ne	ano	ne	ano	ne	ano	ne	ano	ne
12	hlášení událostí	ne	ano	ne	ano	ne	ano	ano	ano	ano

Obrázek 8 Tabulka povinnosti při provozování bezpilotního letounu [63]

Příloha 5

Grafika pro využívání dronů v různých výškách a za různých podmínek



Obrázek 9 Ukázka prostředí ovládání na základě restrikce (GPS) – plánovač a mapa [63]

Příloha 6

Vojenské využití Dronu DJI MAVIC

Obrázek 10 Vojenské využití Dronu DJI MAVIC – drone s připevněnými granáty [64]

Příloha 7

Ukázky opatření proti bezpilotním letounům

Obrázek 11 Střelba sítě z zdronu Falcon na „útočící dron“ [65]

Obrázek 12 Eliminace dronu za pomoci dravce [66]

Obrázek 13 Eliminace dronu dlouhou zbraní [67]

Obrázek 14 Platforma pro střely typu patriot, která byla použita k sestřelení dronu[68]

Příloha 8

Ukázky bezpilotních letounů

Obrázek 15 Bezpilotní letoun typu Reaper MQ-9 [69]